FATF

Update: COVID-19-related Money Laundering and Terrorist Financing

December 2020

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2020), *Update*: *COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses*, FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/update-covid-19-ML-TF.html

Table of Contents

Acronyms

AML/CFT	Anti-money Laundering/Countering the Financing of Terrorism
BRL	Brazilian Real
CHF	Swiss Franc
CTAF	Financial Intelligence Unit of Tunisia
DKK	Danish Krone
ETB	Ethiopian Birr
EUR	Euro
EUROJUST	The European Union Agency for Criminal Justice Cooperation
EUROPOL	The European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigations
FIU	Financial Intelligence Unit
HKD	Hong Kong Dollar
INTERPOL	The International Criminal Police Organization
PEP	Politically Exposed Person
PPE	Personal Protective Equipment
PPP	Paycheck Protection Program
RMB	Chinese Ren Min Bi
SGD	Singapore Dollar
TND	Tunisian Dinar
USD	United States Dollar
VA	Virtual Asset
VAT	Value Added Tax
WHO	World Health Organization

Introduction

The World Health Organization (WHO) declared the COVID-19 outbreak an international pandemic in March 2020. Since then, the pandemic has had an unprecedented impact on peoples' lives around the world. Countries have responded by imposing a variety of public health measures, and implementing stimulus programmes to help protect individuals and companies. These measures have evolved over the last six months, in response to the changing situation in different countries.

Changes in behaviour as a result of the pandemic - whether the behaviour of individuals, companies or governments – have in turn presented criminals with new opportunities to commit crimes and launder the proceeds. The FATF has been monitoring these changes in criminal activity, their impact on anti-money-laundering/counter-terrorist-financing (AML/CFT) regimes, and the measures that governments have implemented to respond to the different types of challenges presented. This has included the publication of a paper in May on COVID-19 risks and policy responses, supplemented by a series of webinars with participants from both the public and private sectors.[1]

Since May, the FATF has continued to collect and assess relevant information on the impact of the pandemic. This assessment confirms that the risks and policy responses published by the FATF in May remain relevant. The purpose of this paper is to provide reporting entities, other private sector entities, and other stakeholders with additional information on COVID-19 related money laundering and terrorist financing risks.

This paper addresses both changes in predicate offences and changes in money laundering and terrorist financing activity. Selected case studies, displaying criminal activity that has occurred since the beginning of the pandemic, highlight the changes in criminal activity. A longer list of case studies provided by jurisdictions around the world is attached as an Annex.

1 The first two webinars, "COVID-19 and the Changing Money Laundering and Terrorist Financing Risk Landscape" and "The Impact of COVID-19 on the Detection of Money Laundering and Terrorist Financing", can be found here and here respectively.

COVID-19-Related ML/TF Risks

Predicate Offences

FATF analysis demonstrates that criminals are continuing to exploit the opportunities created by the pandemic across the globe, with mounting cases of the counterfeiting of medical goods, investment fraud, adapted cyber-crime scams, and exploitation of economic stimulus measures put in place by governments. There have also been examples of online child exploitation due to an increase in the time spent online, increases in property crime due to properties being left uninhabited, and corruption in relation to contracts for medical supplies.

While it is difficult to determine whether criminal activity has increased overall as a result of the pandemic, and while the nature of the risks vary between jurisdictions, a number of jurisdictions have reported dramatic increases in the numbers of particular types of cases. For many jurisdictions, these increases appear to relate to certain types of fraud, such as counterfeiting of medical goods and abuses of economic stimulus measures or corruption relating to public contracts. The example below from Brazil [Case Study 1] provides an example of the increases in particular types of offences as a result of the pandemic, and the measures that authorities have taken to investigate and disrupt the criminal activity.

Case Study 1. Brazil: COVID-19, Organised Crime and Rises in Predicate Offending

In Brazil, between April and November 2020, the Federal Police carried out 56 police operations in 17 different states of the Federation related to acts of corruption or misapplication of public resources and money laundering. These operations concluded with 133 arrests, 985 search and seizure orders and seizure orders in a range of public contract fraud cases, which together amount to approximately BRL 1.9 billion (approx. USD 360 million). The operations varied in size and breadth. For example, in May, in the States of Sao Paulo and Rio de Janeiro, Operation "Placebo" involved public contracts in the amount of BRL 835 million (approx. USD 160 million). Meanwhile, on 29 September in the State of Pará, Operation "S.O.S." involved BRL 500 million (approx. USD 95 million) worth of public contracts.

The cases involved:

- overpricing of the sale of medical equipment to the detriment of public accounts and society,
- purchases of unlicensed medical equipment,
- irregularities in the bidding waiver contracts for the acquisition of respirators,
- general fraud in public tenders and embezzlement of funds destined to combat COVID-19,
- misuse of public resources to combat the pandemic,
- fraud in contracts for the acquisition of hand gels and masks, medications and diagnostic tests for COVID-19, and
- irregularities in the direct contracting of cleaning, disinfection and asepsis services to combat COVID-19.

Some investigations include investigations into money laundering, in addition to the misapplication of public resources, corruption, fraud, embezzlement and other possible predicate offences. The money laundering practices involved the use of bank accounts of third parties and companies, concealment of values in cash, investment in cattle markets, as well as other practices.

Source: Cooperação Jurídica Internacional em Matéria Penal, Brazil (2020)

Counterfeiting Medical Goods

INTERPOL, Europol and others, consider the counterfeiting of medical goods, such as fake medicine and protective clothing, a significant threat.[2] The range of case studies provided to the FATF by delegations from across the Global Network, as well as the frequency of reporting of this typology as a key risk, suggests that the counterfeiting of medical goods

2 For more information, see www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19 and www.europol.europa.eu/newsroom/news/viral-marketing-counterfeits-in-time-of-pandemic respectively.

continues to be a particularly common offence, with jurisdictions from every region around the world reporting increases. The impact of these crimes is particularly significant. Faulty or unregulated medical material has the potential to cause physical harm to the individuals using it.

Case Study 2. Interpol: Exposing International COVID-19 Fraud

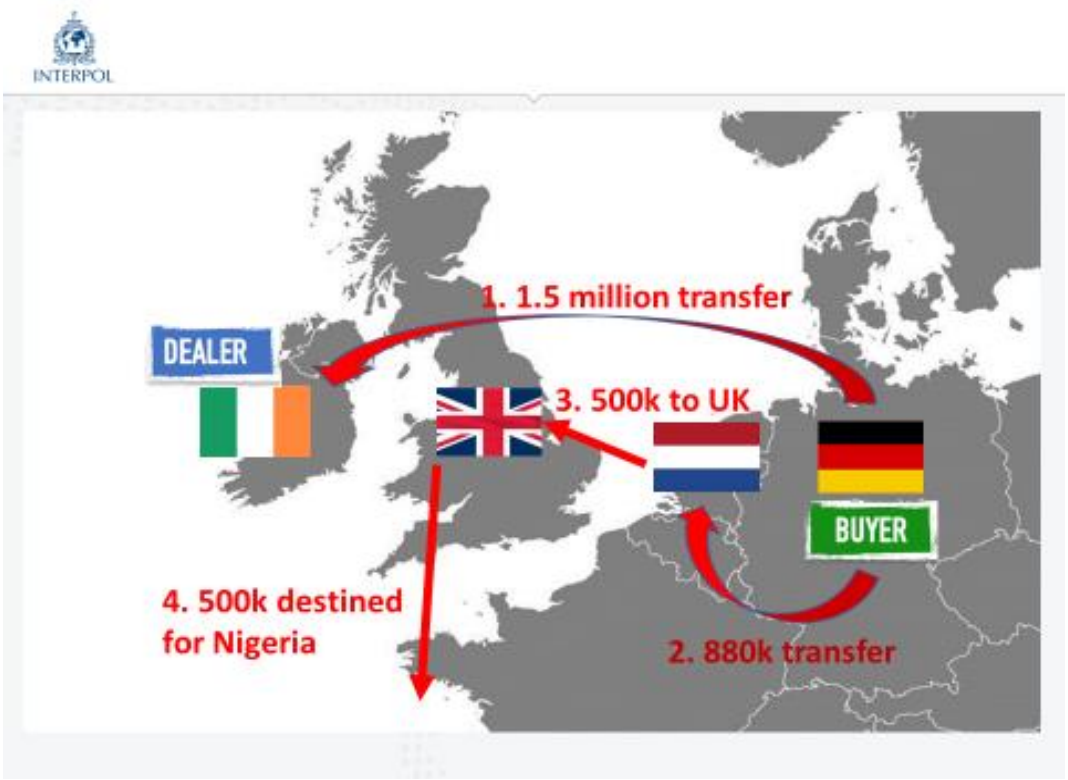
In March, German health authorities contracted two companies in Zurich and Hamburg to procure EUR 15 million worth of face masks. As the global shortage of medical supplies made it difficult to pursue the usual procurement channels, the buyers sought new vendors and found an email address and website which appeared to be linked to a company in Spain. Unbeknownst to them, the site was fake and the email addresses on it were compromised.

The company initially claimed to have 10 million masks, only for the delivery to fall through. It then referred the buyers to a dealer in Ireland who put them in touch with a supplier in the Netherlands. An agreement for an initial delivery of 1.5 million masks was made with the Dutch supplier, requiring an up-front payment of EUR 1.5 million. Just before the delivery date, the buyers were informed that a further transfer of EUR 880 000 was required.

When the buyers realised they were being scammed, they contacted their bank in Germany, which in turn contacted INTERPOL's Financial Crimes unit. Banks, financial intelligence units and judicial authorities, as well as partner organisations Europol and EUROJUST, joined INTERPOL in the investigation. Prompt intervention allowed them to freeze EUR 1.5 million and identify the Irish company involved. The Dutch authorities traced the EUR 880 000 which had been transferred from the German bank. Nearly EUR 500 000 had already been sent to the United Kingdom, all of which was destined for an account in Nigeria.

Thanks to an alert raised by investigators, the UK bank was able to recall the full amount. Those funds have now been returned to the Netherlands and frozen by the authorities. The operation has led to the arrest and sentencing of two suspects in the Netherlands. As per the current findings of the investigations, the two perpetrators were acting on behalf of the main suspect, who was arrested in August in Nigeria.

Figure 1. International COVID-19 Scam



Source: Interpol (2020)

Examples submitted by jurisdictions suggest that schemes involving the sales of counterfeited medical goods, or non-delivery scams, can be both domestic and international in nature – such as the multination case above [Case Study 2] or the domestically focused case below [Case Study 3]. These scams may involve personal protective equipment, pharmaceutical products or other types of medical equipment, for which there has been a substantial increase in demand.

Case Study 3. Hong Kong, China: Domestic Personal Protective Equipment Fraud

In January 2020, an individual posted an advertisement on various e-commerce platforms claiming to have a large quantity of surgical masks and alcohol sanitisers for sale. Between January and March 2020, more than 200 victims purchased these goods locally and paid for them by depositing cash or making electronic fund transfers. A total of HKD 1.4 million (USD 180 630) was deposited into three Hong Kong bank accounts and four e-wallets held by the individual's spouse and their associates.

In early March 2020, victims reported that they had not received their goods and were unable to get in touch with either of the individuals involved. Investigations revealed that the money was withdrawn quickly after victims deposited it into the designated bank accounts and e-wallets.

Law enforcement arrested four individuals in April 2020. At the time of publication of this report, the individuals have not been charged and the investigation remains ongoing.

Source: Financial Services and the Treasury Bureau, Hong Kong, China (2020)

Cybercrime

A significant number of jurisdictions from various regions around the world report a continued increase in cyber-related scams, in particular email and SMS phishing schemes [Case Study 4], business email compromise scams [Case Study 5] but also ransomware attacks.

As governments' actions and individuals' interests have changed over the last six months, the COVID-19–related SMS and email phishing schemes have shifted. These now include emails with fake links to government stimulus packages, banks distributing aid, infection rate maps, and websites selling masks. One jurisdiction reported a case where criminals sent emails threatening not only to divulge personal data of victims, but also to infect them and their families with the coronavirus if they did not pay the criminals.

Case Study 4. Spain: Email Phishing Campaigns

The cybercrime department of the National Police from Spain received an alert of a phishing attack involving a large number of emails impersonating a well-known online retailer company. These phishing attacks focused on obtaining identification information of the victims and their credit card numbers. The data obtained from the victims could then be sold to other criminal organizations or used in further fraudulent activities. This incident took place at the beginning of the pandemic during the first lockdown period, at the end of March, when there were severe limitations on movement and an increase in the volume of online purchases (and consequently an increase in phishing attacks).

The content of the email messages indicated that the personal account of the customer in the aforementioned company had been blocked for security reasons due to possible non-legitimate access. A link to a webpage posing as the online retail company was also included in the email with the aim of fraudulently obtaining information.

The illicit activity was detected through the analysis of information and data transactions developed by the specialized cybercrime police units. Due to increased online activity in the lockdown period these units engaged in enhanced monitoring or so-called 'cyber patrolling'. The crime was linked to local Spanish speaking victims due to the language of the emails. The case remains under investigation.

Source: Financial Intelligence Unit, Spain (2020)

Case Study 5. Singapore and France: International Business Email Compromise Scam

In March 2020, a Singapore-based bank raised an alert after it received a funds recall message from a French company. The bank notified the Singapore authorities of its suspicion and, given the international component to the transaction, Singapore authorities immediately notified their French counterparts of the suspicious money flow and possibility of fraud. Through quick intervention and collaboration with banks, the Commercial Affairs Department of the Singapore Police Force seized over SGD 6.4 million (EUR 4 million) on the same day of the alert.

The ensuing investigation found that a French pharmaceutical products company was the victim of a fraud involving false transfer orders for a total loss of EUR 6.64 million. The company had fulfilled an order for surgical masks and hand hydro-alcoholic gel from their usual suppliers, whose identity was stolen through a business email compromise scam. The French company was deceived into transferring EUR 6.64 million to a Singapore-based bank account owned by the fraudsters, after which the company neither received the products nor could reach the supplier.

Later in March 2020, a 39-year-old man was arrested in Singapore on suspicion of laundering scam proceeds relating to COVID-19 medical supplies of SGD 10.2 million (EUR 6.64 million). The individual has not been charged as of yet. He was found to be acting in concert with an organized crime group based overseas. The Singapore authorities continue to work with the French authorities on the case.

Source: Singapore Police Force, Ministry of Economy and Finance, France (2020)

Investment Fraud

Jurisdictions in most regions continue to report risks of investment fraud involving the fraudulent advertising of companies that are supposedly developing so-called "miracle cures" to COVID-19. Scammers have attracted victims by making false claims that their investment will exponentially grow in value as a result of the pandemic, with the funds then withdrawn and laundered by the criminals operating the scheme.

Case Study 6. California, United States of America: Investment Fraud

In June 2020, a man in California was indicted on fraud charges alleging that he solicited people around the nation to invest in companies that would market pills he claimed would prevent coronavirus infections and produce an injectable cure for those already suffering from COVID-19.

The defendant falsely claimed to have developed a cure for the COVID-19 virus and a treatment that prevented a person from being infected by the COVID-19 virus through text messages, videos, and statements sent to potential investors and posted on the internet. The indictment alleges that he fraudulently solicited investments in two companies with a series of false promises, including miraculous results from the prevention product and the cure, and risk-free and 100 percent guaranteed "enormous returns" on investments. To bolster the claims, the defendant falsely represented that an unnamed party in Dubai had offered to purchase the two companies for USD 10 billion, claiming this offer would secure the victim-investors' investments in the two companies, and that he had secured funding from seven investors who had each already invested between USD 750 000 and USD 1 000 000.

The FBI arrested the defendant in March 2020 after he delivered pills – purportedly the treatment that prevents coronavirus infection – to an undercover agent posing as an investor. He has been charged with 11 counts of wire fraud stemming from solicitations he allegedly made to potential investors in Nevada, New York, Texas and Colorado. Two of the charges relate to communications with the undercover agent.

Note: In the United States, an indictment contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt.

Source: Department of Justice, United States of America (2020)

Charity Fraud

Fraud through fundraising for fake charities has continued throughout the pandemic. In these schemes, scammers contact individuals, misrepresent themselves and seek money for a non-existing charity, or make use of social media platforms to appeal for funds. In some instances, fraudsters have deceived victims by acting as if they were representatives of well-known global charities, and in other instances they have created fake charities.

Case Study 7. China: Charity Fraud Scam Case Study Placeholder

Mr. W, claiming to donate towards the fight against COVID-19, published donation information with a fund-raising QR code on an online platform, calling for public donations. During the pandemic, over 100 people from all over China paid in by scanning the QR code, mostly integral multiples of RMB 10 (USD 1.50) or RMB 100 (USD 15). The total value of donations exceeded RMB 100 000 (USD 14 960). Shortly after the money was credited, it was transferred to Mr. W's personal bank account. There was no corresponding donation record, only obvious features of fraudulent actions. The case has been reported to the police for investigation and no connection between the offender and organized criminal groups has been found as of yet.

Source: Anti-Money Laundering Bureau, The People's Republic of China (2020)

Abuse of Economic Stimulus Measures

The abuse of economic stimulus measures has continued to evolve. Over the last six months, countries have implemented an increased number and increased sizes of stimulus programmes. This has provided criminals with opportunities, and resulted in cases where individuals, companies, or organised criminal groups attempt to fraudulently claim money from governments.

Case Study 8. Washington, United States of America: Abuse of Economic Stimulus Measures and Money Laundering

In July 2020, a tech executive in the state of Washington was charged with one count of wire fraud and one count of money laundering in connection with the alleged submission of at least eight fraudulent Paycheck Protection Program (PPP) loan applications on behalf of six different companies to federally insured financial institutions. The applications sought more than USD 5.5 million in loans. In support of the fraudulent loan applications, the individual allegedly made numerous false and misleading statements about the companies' respective business operations and payroll expenses. The criminal complaint further alleges that he submitted fake and altered documents, including fake federal tax filings and altered incorporation documents.

For example, the individual allegedly misrepresented that one of his companies had dozens of employees and paid millions of dollars in wages and payroll taxes. The company, purchased on the internet in May 2020, actually had no employees and no business activity at the time of the purchase. The individual also allegedly transferred at least USD 231 000 in fraudulently obtained loan proceeds to his personal brokerage account for his personal benefit. This case was investigated by the Federal Housing Finance Agency's Office of Inspector General, the Internal Revenue Service-Criminal Investigation, the U.S. Treasury Inspector General for Tax Administration, and the Federal Deposit Insurance Corporation's Office of Inspector General.

Note: In the United States, a criminal complaint is merely an allegation and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Source: Department of Justice, United States of America (2020)

Case Study 9. Switzerland: Fraudulent COVID-19 Loan Applications

In mid-June 2020, a financial institution granted a COVID-19-loan of around of around CHF 90 000 (EUR 98 500) to a company active in the construction sector. A few days later, the financial institution was informed that the same company sought an additional loan from another financial institution. In the meantime, most of the original loan was withdrawn in cash or spent for daily consumption expenses. The financial institution therefore filed a suspicious activity report and provided it to the Swiss FIU. The case has been forwarded to the competent Swiss law enforcement authorities where criminal proceedings are currently ongoing.

Source: Federal Department of Finance. Switzerland (2020)

Case Study 10. Italy: Organized Crime and Abuse of Economic Stimulus Measures

Investigations ending in July 2020 revealed that members of a criminal group, linked to a mafia-style organised crime group ("*ndrangheta*"), were running a business purportedly involved in the trading of metals in Italy. However, the business was in fact dedicated to the commission of a number of predicate offences involving COVID-19.

The predicate offences involved producing false or misleading tax statements, which were used to fraudulently obtain VAT refunds. The funds were then laundered using banks and the money or value transfer systems. Part of the money was sent to a company located in a foreign country in Europe, another part was sent to a foreign country overseas and the criminals received the correspondent amount in cash in Italy.

The VAT fraud generated a false turnover for companies involved into this scheme. In the context of the COVID-19 pandemic, it created the requisite to get public non-repayable grants. The criminal scheme was also used to attempt to request additional economic support.

Further investigations revealed that the main suspect used the false turnover generated by the VAT fraud to falsely justify losses due to the pandemic, in order to receive non-repayable grants awarded as COVID-19 countermeasures for three companies included in the criminal scheme. Investigations also detected the criminal attempted to benefit from state-granted loans in the context of measures aimed at supporting the economic system following the COVID-19 emergency. Law enforcement authorities seized nearly EUR 7.5 million worth of assets and financial resources and executed 10 arrests.

Source: Guardia di Finanza, July (2020)

In addition to the misuse of government funds involving fraudulent enterprise loans, grant applications and unemployment insurance applications, a number of jurisdictions have also expressed concerns over the possible misappropriation of international aid received for the purpose of battling the pandemic. In addition, several jurisdictions also reported cases of corruption involving the misuse of government funds intended for the use of medical equipment or publicly funded contracts.

Case Study 11. Tunisia: Misappropriation of Aid

In October 2020, the financial intelligence unit of Tunisia (CTAF) received a suspicious transaction report from a financial institution indicating that a Tunisian citizen (Mr. X) cashed in a TND 2 million bank cheque (approx. USD 724 000) into the account of his firm, Company C. Mr. X claimed that the consulate of a foreign country issued the cheque to him. It allegedly intended to provide 2 000 foreign citizens stranded in Tunisia during the containment period with accommodation, medicines, supplies and COVID-19 tests.

On the same day that Mr. X cashed the cheque, he transferred the entire amount to different accounts held by natural persons, clinics and his brother's firm, Company A. Shortly after, the CTAF received another suspicious transaction report from a different financial institution, which was triggered by the fact that the account of Company A received five identical wire transfers from Company C on the same day totalling TND 400 000 (USD 145 000).

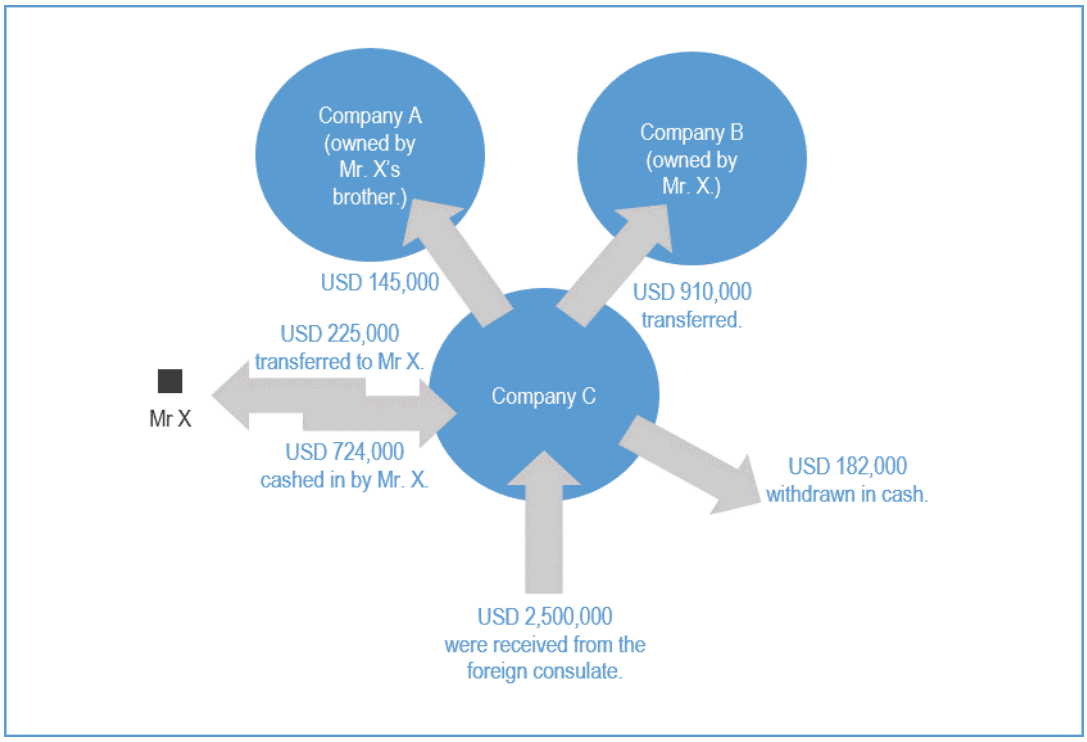
Further analysis showed that within a short time span (less than 6 months after opening the account) Company C received six wire transfers only from the mentioned consulate for a total amount of almost TND 7 million (USD 2.5 million). Shortly after, TND 500 000 (USD 182 000) were withdrawn in cash, TND 2.5 million (USD 910 000) were transferred to Company B's account (owned by Mr. X), and TND 700 000 (USD 255 000) were transferred to Mr. X's personal account.

Mr. X spent only 15% of the sum received from the foreign consulate on hotels, clinics and pharmacies. The contract between the consulate and Company C, did not define the services required from the company, the prices, or the taxes involved. Further, Company C has no other bank accounts or economic activity. Meanwhile, transfers sent to Company A were found to be based on fraudulent invoices, containing abnormally high prices compared to those normally charged.

Consequently, CTAF concluded that Mr. X used a shell company (Company C), family companies and fraudulent invoices to misdirect public aid given by a foreign country to its citizens stranded in Tunisia because of the COVID-19 pandemic The CTAF ordered, as a preventive measure, a freezing of the accounts of companies A, B and C, and Mr. X's bank account. The CTAF sent a spontaneous disclosure to the foreign financial intelligence unit and transmitted the report to the prosecutor. The investigation is ongoing.

Source: Financial Intelligence Unit, Tunisia (2020)

Figure 2. Tunisia: Misappropriation of Aid



Source: Financial Intelligence Unit, Tunisia (2020)

Money laundering and terrorist financing risks

As the impact of the COVID-19 pandemic continues, the money laundering risks are likely to become clearer over the coming months. Nevertheless, jurisdictions continue to see some of the vulnerabilities identified earlier in the year by the FATF as a result of the pandemic.

Vulnerabilities revolve around changing financial behaviours, in particular a rise in remote transactions, with impacts on financial institutions' ability to detect anomalies. With increasing unemployment, and larger numbers of citizens conducting transactions remotely, there are also risks that vulnerable citizens will be exploited as money mules.

Other vulnerabilities relate to increased financial volatility caused by the global economic downturn triggered by confinement measures to curb the spread of COVID-19. These include increased amounts of cash in circulation, and the use of virtual assets.

Many jurisdictions have not identified a change in the terrorist financing risks as a result of the pandemic, although some noted potential future vulnerabilities. These relate to the misuse of non-profit organisations and new opportunities in relation to the predicate threat environment.

Changing Financial Behaviours

Changes in customer behaviour are continuing to make it more difficult for financial institutions to identify anomalies. Customers' financial patterns, for example, are changing as they work from home and conduct more online transactions. In some countries, where remote transactions and services are less frequently used, reporting entities may not yet be accustomed to facilitating transactions or offering services remotely. This makes it more difficult for them to conduct effective customer due diligence or ongoing monitoring. In some

cases, moves to remote working have impacted the effectiveness of reporting entities' systems and controls, with compliance staff unable to carry out their functions with the same efficiency as they would have done before the pandemic.

The effective use of technology, whether used to support on-boarding or to ensure effective information sharing between competent authorities and reporting entities, has become even more important as customers' behaviour changes and social distancing measures mean that face-to-face interaction isn't always possible.

The evolving risk landscape also means risk indicators need to be regularly updated and adjusted, and effective ongoing communication between the public and private sectors is needed to share information as the risks change over time.

Case Study 12. Abuse of Dormant Accounts in Ethiopia

A bank employee illegally withdrew ETB 3 million (EUR 68 300) from an inactive customer account and lent it to his friend without any collateral. When the internal auditors of the bank discovered the illegal withdrawal of money from the inactive account, they reported the case to the Ethiopian Financial Intelligence Centre as a suspicious transaction. The Centre then conducted analysis and sent the results to law enforcement authorities for further criminal investigation. Both the bank employee and the individual who received the money are under investigation. They have been charged with corruption and other related financial crimes and temporarily released from custody on bail. The case is still active.

This offence occurred during a state of emergency declared in Ethiopia to contain COVID-19. Due to the measure, only 50% of employees were working in the bank while the rest were working from home. This allowed the employee to exploit the system and commit the crime. In addition, many businesses were continuously inactive during the state of emergency. Both scenarios created vulnerabilities. Further, the control systems in financial institutions were weaker due to the reduction in the number of employees physically present at the banks to perform know-your-customer, customer due diligence measures, etc.

Source: Ethiopian Financial Intelligence Center (2020)

Increased Financial Volatility and Economic Contraction

Many jurisdictions are facing economic contraction and this is also resulting in a number of vulnerabilities for money laundering. One risk is that funds from illicit sources can be used to exploit businesses in distress or subject to rapid changes in demand through the provision of capital or a take-over. Real estate, construction, industrial cleaning, and transportation sectors, as well as small and medium enterprises in general, appear to be particularly vulnerable.

Meanwhile, concerns about the economy have led to an increase in cash-withdrawals and a growing amount of cash the circulation. Combined with the closing of borders and

restrictions on individuals' movements, this has increased criminal groups' use of fiat currency to store cash and launder the proceeds of their crimes.

Other vulnerabilities include individuals turning to unregulated financial services, and scams to appeal to individuals who may have lost their jobs or suffered a loss in income, including potentially being exploited as money mules. Increased financial volatility also poses a vulnerability for insider trading, where large shifts of value as a result of the pandemic may create opportunities to commit insider trading.

Tied to increased financial volatility, there may be additional vulnerabilities linked to the misuse of virtual assets (VAs) in pandemic-related schemes (e.g. VAs may be used for payments in fraud schemes linked to the pandemic). This is largely because like with cash (as above), stockpiling of VAs increases when there are general concerns over the state of the economy.

Competent authorities noted further concerns around VAs, including money mule scams that target the recently unemployed or furloughed. In one typology, criminals, posing as fake employers, approach their victims asking them to accept a "donation" into their own bank account and to deposit the funds into a crypto kiosk. If the funds are illicit, the victim unwittingly accepts to partake in money laundering acting as a money mule.

Case Study 13. Hong Kong, China: Virtual Assets and COVID-19 Fraud

Between late February and early March 2020, an owner of a health-care products trading company in Hong Kong, China saw internet advertisements posted by several purported sellers of surgical masks and medical equipment, including on a major social media platform. When she attempted to purchase the equipment, she was deceived into transferring HKD 450 000 (USD 58 000) to various bank accounts in Hong Kong, China and an Eastern European country and into converting the equivalent of HKD 3.96 million (USD 510 000) into Bitcoin. To do so, the victim withdrew cash from her personal bank account and deposited the cash to a designated Bitcoin ATM where the funds were transferred to designated Bitcoin accounts. In total, three banks located in two jurisdictions (Hong Kong, China and an Eastern European jurisdiction) were involved. Five transfers ranging from USD 47 250 to USD 235 830 worth of Bitcoins were transferred to accounts owned by the culprit. All of the scammers stopped responding to the victims after receiving the payment. The investigation is ongoing.

Source: Financial Services and the Treasury Bureau, Hong Kong, China (2020)

Conclusion

The impacts of the pandemic continue to evolve. Consequently, the changes in both money laundering and terrorist financing activity as a result of the pandemic are likely to continue to evolve as well. Rising unemployment, financial distress, the bankruptcy of companies, the increased circulation of cash in economies, potential stockpiling of cash by organised criminal groups, and the accelerated implementation of stimulus programs represent vulnerabilities that criminals may increasingly exploit over the coming months. Furthermore, as the development of new COVID-19 vaccines accelerate, so too will opportunities for criminals to devise criminal scams to exploit and illegally profit from these new medical advancements.

While there are some globally consistent trends, other risks may be specific to particular countries or regions. The FATF will continue to monitor the impact of the pandemic on global ML and TF risks and on AML/CFT regimes, working closely with observer organisations and the network of FATF-Style Regional Bodies to understand regional specificities. The FATF will provide further updates, should the impacts significantly evolve.

It continues be critical for jurisdictions, financial institutions, and designated non-financial business and professions to identify, assess, and understand the particular ML and TF risks they face, and take corresponding mitigating action in line with the FATF Recommendations.

If you have feedback on this report or the FATF's response to the COVID-19 pandemic please contact secretariat@fatf-gafi.org.

COVID-19 Case Studies Long List

List of COVID-19-Related Case Studies of ML/TF Risks including cases included within the body of the report

Many of these cases are ongoing. Unless indicated otherwise, the charges in some of these cases are only accusations of a crime, and those charged with a penal offence have the right to be presumed innocent until proved guilty according to law in a public trial.[3]

This list is not to be considered an exhaustive one of all COVID-19-related case studies exhibiting ML/TF risks. It is a snapshot of the currently available case studies on this topic that have been disclosed for publication.

Type of Case	Jurisdiction(s) Involved	Description
Organised Crime	Brazil	In Brazil, between April and November 2020, the Federal Police carried out 56 police operations had been carried out by the Federal Police in 17 different states of the Federation related to acts of corruption or misapplication of public resources, in addition and to money laundering. These operations concluded with 133 arrests, 985 search and seizure orders, and contractual fraud, which together amount to approximately BRL 1.9 billion (approx. USD 400 million). The operations varied in size and breadth. For example, on 25 May, in the States of Sao Paulo and Rio de Janeiro, Operation "Placebo" involved public contracts in the amount of BRL 835 million (approx. USD 170 million). Meanwhile, on 29 September in the State of Pará, Operation "S.O.S." involved public contracts in the amount of BRL 500 million (approx. USD 100 million) worth of public contracts. The cases involved: • overpricing of the sale of medical equipment to the detriment of public accounts and society, • purchases of unlicensed medical equipment, • irregularities in the bidding waiver contracts for the acquisition of respirators, • general fraud in public tenders and embezzlement of funds destined to combat COVID-19, • misuse of public resources to combat the pandemic, • fraud in contracts for the acquisition of hand gels and masks, medications and diagnostic tests for COVID-19, and • irregularities in the direct contracting of cleaning, disinfection and asepsis services to combat COVID-19. Some investigations money laundering practices, in addition to the misapplication of public resources, corruption, fraud, embezzlement and other possible predicate offences, in some investigations money laundering practices were identified. The money laundering practices involved the use of bank accounts of third parties and companies, concealment of values in cash, investment in cattle markets and others. Case Study 1 *Source: Cooperação Jurídica Internacional em Matéria Penal, Brazil (2020)*
Counterfeiting Medical Goods – PPE Fraud	Germany, Spain, Netherlands, Ireland, United Kingdom, Nigeria	In March, German health authorities contracted two companies in Zurich and Hamburg to procure EUR 15 million worth of face masks. As the global shortage of medical supplies made it difficult to pursue the usual procurement channels, the buyers sought new vendors and found an email address and website which appeared to be linked to a company in Spain. Unbeknownst to them, the site was fake and the email addresses on it were compromised. The company initially claimed to have 10 million masks, only for the delivery to fall through. It then referred the buyers to a dealer in Ireland who put them in touch with a supplier in the Netherlands. An agreement for an initial delivery of 1.5 million masks was made with the Dutch supplier, requiring an up-front payment of EUR 1.5 million. Just before the delivery date, the buyers were informed that a further transfer of EUR 880 000 was required.

3 In accordance with the Universal Declaration of Human Rights (1948). See here.

Type of Case	Jurisdiction(s) Involved	Description
		When the buyers realised they were being scammed, they contacted their bank in Germany, which in turn contacted INTERPOL's Financial Crimes unit. Banks, financial intelligence units and judicial authorities, as well as partner organisations Europol and EUROJUST, joined INTERPOL in the investigation. Prompt intervention allowed them to freeze EUR 1.5 million and identify the Irish company involved. The Dutch authorities traced the EUR 880 000 which had been transferred from the German bank. Nearly EUR 500 000 had already been sent to the United Kingdom, all of which was destined for an account in Nigeria. Thanks to an alert raised by investigators, the UK bank was able to recall the full amount. Those funds have now been returned to the Netherlands and frozen by the authorities. The operation has led to the arrest and sentencing of two suspects in the Netherlands. As per the current findings of the investigations, the two perpetrators were acting on behalf of the main suspect, who was arrested in August in Nigeria. Case Study 2 *Source: Interpol (2020)*
Counterfeiting Medical Goods – PPE Fraud	Hong Kong, China, Republic of Korea	The victim was attempting to procure surgical masks via an online advertisement on Instagram during the early stages of the pandemic when many were instilled with a sense of fear with regards to medical equipment shortages amid COVID-19. The victim began to engage with the fraudster who asked for an advance payment to secure the order. The victim sent EUR 54 250 to a Korean bank account as per the instructions from the fraudster. After that the seller cut all communication with the victim. The case was reported to law enforcement who alerted the INTERPOL National Central Bureau (NCB) in Hong Kong. INTERPOL Hong Kong sent a request to INTERPOL Seoul to help this investigation in February. The FIUs in each respective country were also contacted to assist who in turn liaised with the relevant financial institution. Due to the swift interaction of all actors involved, two suspects were arrested 4 days after the victim lodged the initial report and the full amount of money returned to the victim's account. *Source: Interpol (2020)*
Counterfeiting Medical Goods – PPE Fraud	Italy, Indonesia	In May 2020, an Italian company was in discussions with a Chinese company to purchase a large amount of medical supplies, including ventilators and COVID-19 monitoring equipment. Individuals with criminal intent, infiltrated the email correspondence between the two companies and convinced the Italian buyers to make three bank transfers totalling EUR 3.67 million to an account they controlled in Indonesia. Under the assumption that this was a legitimate supplier, the Italian company made the transfers. The fraud was discovered when the supplier in China informed the Italian victim company that it had not received the payments for the medical equipment purchased. Further checks showed that there was an intrusion into the email correspondence that led to the diversion of funds to the bank account in Indonesia. Accordingly, the victim company lodged a police report with the Italian authorities. The assistance of INTERPOL's Financial Crime Unit was requested via the NCB Rome. INTERPOL facilitated the connection with Indonesian authorities through its global network. Law enforcement contacted the FIU's in each jurisdiction and the financial institutions. Connecting the relevant actors within the financial AML arena quickly led to the interception and freezing of EUR 3.1 million of the fraudulent payments in early June. To further support the investigation, in August, INTERPOL held a virtual case coordination meeting with the key stakeholders in Italy and Indonesia including the INTERPOL NCB in Rome, the Italian Postal Police Service, the National Central Bureau in Jakarta well as the Financial Intelligence Unit and the Criminal Investigation Department of Indonesia. They all shared critical investigative details and worked together to secure the frozen assets and locate the suspects behind the fraud. Following the meeting, Indonesian authorities identified the three suspects, who were part of a wider criminal network involved in the fraud. They were arrested in early September at which time police also seized cash and assets allegedly purchased using the stolen money. Investigations continue into the activities of the criminal syndicate to determine if there have been other victims from other countries. *Source: Interpol (2020)*

Type of Case	Jurisdiction(s) Involved	Description
Counterfeiting Medical Goods – PPE Fraud	Hong Kong, China	In January 2020, an individual posted an advertisement on various e-commerce platforms claiming to have a large quantity of surgical masks and alcohol sanitisers for sale. Between January and March 2020, more than 200 victims purchased these goods locally and paid for them by depositing cash or making electronic fund transfers. A total of HKD 1.4 million (USD 180 630) was deposited into three Hong Kong bank accounts and four e-wallets held by the individual's spouse and their associates. In early March 2020, victims reported that they had not received their goods and were unable to get in touch with either of the individuals involved. Investigations revealed that the money was withdrawn quickly after victims deposited it into the designated bank accounts and e-wallets. Law enforcement arrested four individuals in April 2020. At the time of publication of this report, the individuals have not been charged and the investigation remains ongoing. Case Study 3 *Source: Financial Services and the Treasury Bureau, Hong Kong, China (2020).*
Counterfeiting Medical Goods – PPE Fraud	Germany	At the end of February 2020, a German company ordered a large quantity of protective masks from a supplier in a non-EU country. A down payment of a high six-digit euro amount was transferred to the seller in the corresponding non-EU country (approximately 50% of the purchase price). However, no delivery was made. The German company did not receive any response to any attempts of contact. The FIU in Germany then received an urgent request from a law enforcement agency. Following the request, the German FIU immediately sent a request for information to the FIU of the non-EU country with the additional request to freeze the funds or to block the account of the beneficiary. The FIU of the non-EU country froze the funds on the same day. The German FIU was informed of the frozen funds and direct contact was then made with the law enforcement agency in Germany and the FIU liaison officer based there. The public prosecutor's office thereupon obtained an arrest of assets, which was channeled by means of judicial administrative and legal assistance requests through the regular judicial channels provided for this purpose. In addition, the arrest of assets was also transmitted to the FIU in the non-EU country. *Source: Federal Ministry of Finance, Germany (2020)*
Counterfeiting Medical Goods – PPE Fraud	Luxembourg	In March 2020, the FIU Luxembourg received an urgent request for information in relation with a Luxembourg-based company offering significant quantities of surgical masks for sale to an EU Member State Government. The context of the worldwide COVID-19 pandemic resulting in a shortage of medical and protective equipment, raised doubts regarding the seriousness of the offer and the company involved. Furthermore, doubts were reinforced as the bank account mentioned on the invoice provided by the Luxemburgish company was in a different jurisdiction (Country A). The Luxembourg FIU's preliminary analysis revealed that the company, incorporated in 2013, was a holding company generating no income and holding a single participation in another company of Country B. Besides that, the company had no VAT number and no trading permit. As the company was domiciled within a trust company being a reporting entity, the FIU requested bank statements for further analysis. It turned out that the company only had bank accounts in Country A, but no movements in relation with trading of goods could be identified since the company's incorporation in 2013. FIU Luxembourg has engaged in international cooperation with the FIU of Country A. In addition, the FIU in Luxembourg was informed that the company was in a business sale process and that a potential buyer was identified. As the company had unpaid invoices, the trust company took the decision to terminate the contract and the director of the company resigned. *Source: Financial Intelligence Unit, Luxembourg (2020)*

Type of Case	Jurisdiction(s) Involved	Description
Counterfeiting Medical Goods – PPE Fraud	Malaysia	FIU Malaysia received a request for information from a country in Europe (Country A) concerning a suspected facemask scam amid the COVID-19 pandemic. Approximately EUR 5 million was transferred by a government agency in Country A to an entity in Country A, namely Company ABC for the purchase of facemasks from Country B. It was discovered that only a portion of the facemasks was delivered where all were found to be unfit for hospital use. Financial intelligence gathered by Country A later revealed that Company ABC may have subsequently transferred a significant amount of money intended for facemask purchase to another entity, namely Company XYZ in Malaysia. Further transaction review of the company account also revealed an inward remittance received by Company XYZ from an entity located in Country C with transaction remarks that may potentially indicate facemask related transactions. Within the same day, another large sum of monies amounting to approximately USD 150 000 was received from Company DEF, another entity in Country A, believed to be engaging in sales of healthcare products including gloves, goggles and hearing protection. The funds received by company XYZ were observed to have been disbursed to various entities in Country C and Country D. *Source: Financial Intelligence Unit, Malaysia (2020)*
Counterfeiting Medical Goods – PPE Fraud	Malaysia	FIU Malaysia received a request for information from a country in Europe (Country E) concerning suspected fraud with protective equipment for testing of COVID-19. A national health agency in Country E received a commercial proposal from Company OPQ in Country E, to purchase protective equipment for testing of COVID-19 worth millions of euros. Company OPQ had defrauded the national health agency in Country E into signing a contract for equipment of a higher price by providing false product information. Financial intelligence gathered by Country E later revealed that Company OPQ may have subsequently transferred EUR 6.05 million intended for the purchase of protective equipment for testing of COVID-19 through networks of companies involving companies in Country E and two neighbouring countries and eventually to another entity, namely Company RST in Malaysia. A transaction review of the company account revealed a pattern of rapid and high frequency of incoming and outgoing transactions involving multiple counterparties consisting of inward SWIFT and foreign wire transfers. Further review of the account revealed that Company RST received an inward remittance from Company UVW which was based in one of the neighbouring countries. Funds received were later transferred to entities outside Malaysia via wire transfers. *Source: Financial Intelligence Unit, Malaysia (2020)*
Counterfeiting Medical Goods – PPE Fraud	Finland	A Finnish governmental actor purchased 3.1 million masks for approximately EUR 5 million from a private Finnish company. This company in turn purchased the goods from a vendor in China. However, right after the purchase, it turned out that the private Finnish company's entrepreneur had a questionable business history, and the quality of a major part of the delivered medical supplies were substandard. The FIU discovered the questionable business history during routine checks. There was a lack of tax reporting, outstanding tax debts of the company during past fiscal years, and the company was excluded from certain official databases. The case is still under investigation as an aggravated fraud. However, throughout the investigation authorities have confiscated assets for EUR 2.6 million. *Source: Financial Intelligence Unit, Finland (2020)*
Cyber-crime	Singapore, France	In March 2020, a Singapore-based bank raised an alert after it received a funds recall message from a French company. The bank notified the Singapore authorities of its suspicion and, given the international component to the transaction, Singapore authorities immediately notified their French counterparts of the suspicious money flow and possibility of fraud. Through quick intervention and collaboration with banks, the Commercial Affairs Department of the Singapore Police Force seized over SGD 6.4 million (EUR 4 million) on the same day of the alert.

Type of Case	Jurisdiction(s) Involved	Description
		The ensuing investigation found that a French pharmaceutical products company was the victim of a fraud involving false transfer orders for a total loss of EUR 6.64 million. The company had fulfilled an order for surgical masks and hand hydro-alcoholic gel from their usual suppliers, whose identity was stolen through a business email compromise scam. The French company was deceived into transferring EUR 6.64 million to a Singapore-based bank account owned by the fraudsters, after which the company neither received the products nor could reach the supplier. Later in March 2020, a 39-year-old man was arrested in Singapore on suspicion of laundering scam proceeds relating to COVID-19 medical supplies of SGD 10.2 million equivalent (EUR 6.64 million). The individual has not been charged as of yet. He was found to be acting in concert with an organized crime group based overseas. The Singapore authorities continue to work with the French authorities on the case. Case Study 5 *Source: Singapore Police Force, Ministry of Economy and Finance (France)*
Cyber-crime	Spain	The cybercrime department of the National Police from Spain received an alert of a phishing attack involving a large number of emails impersonating a well-known online retailer company. These phishing attacks focused on obtaining identification information of the victims and their credit card numbers. The data obtained from the victims could then be sold to other criminal organizations or used in further fraudulent activities. This incident took place at the beginning of the pandemic during the first lockdown period, at the end of March, when there were severe limitations on movement and an increase in the volume of online purchases (and consequently an increase in phishing attacks). The content of the email messages indicated that the personal account of the customer in the aforementioned company had been blocked for security reasons due to possible non-legitimate access. A link to a webpage posing as the online retail company was also included in the email with the aim of fraudulently obtaining information. The illicit activity was detected through the analysis of information and data transactions developed by the specialized cybercrime police units. Due to increased online activity in the lockdown period these units engaged in enhanced monitoring or so-called 'cyber patrolling'. The crime was linked to local Spanish speaking victims due to the language of the emails. The case remains under investigation. Case Study 4 *Source: Financial Intelligence Unit, Spain (2020)*
Mobile Phone Fraud	Israel	A regional cyber unit of the Israel National Police has recently conducted an undercover investigation concerning suspected fraud activity amounting to hundreds of thousands of ILS, committed by a group of 16 people, who systematically operated under the organized supervision of a married couple in their mid-40s. The group fraudulently stole an approximate amount of ILS 700 000 (approx. USD 210 000) from dozens of victims, by taking over their mobile phone information using a SIM-Swap scam, hacking into their personal bank accounts using SMS One-Time Passwords (OTPs), and then withdrawing thousands of ILS from the victims' accounts. The investigation began in March 2020, when one of the regional cyber units of the Israel National Police analysed several complaints submitted by citizens, most of them wealthy elderly individuals. The investigation revealed a common fraudulent method used across the country, in which hundreds of bank transfers were made without the consent, or knowledge of the account owners. The covert investigation revealed that the scams were purposefully carried out during the COVID-19 lockdown since the victims (especially the elderly) were unable to leave their homes, or visit the bank, and therefore were unable to track or detect the fraudulent transfers that were made from their bank accounts.

Type of Case	Jurisdiction(s) Involved	Description
		In October 2020 the Israeli National Police arrested 16 suspects, conducted searches of their homes and seized computers and digital storage devices. A collaboration between the Israeli National Police and the Israeli FIU (IMPA) revealed outgoing international wire-transfers. An information request was sent to the foreign FIU in order to trace and seize the funds. An indictment against the two main suspects was filed on 9 November 2020. *Source: Israel Money Laundering and Terror Financing Prohibition Authority, IMPA (2020)*
Charity Fraud	China	Mr. W, claiming to donate towards the fight against COVID-19, published donation information with a fund-raising QR code on an online platform, calling for public donations. During the pandemic, over 100 people from all over China paid in by scanning the QR code, mostly integral multiples of RMB 10 (USD 1.50) or RMB 100 (USD 15). The total value of donations exceeded RMB 100 000 (USD 14 960). Shortly after the money was credited, it was transferred to Mr. W's personal bank account. There was no corresponding donation record, only obvious features of fraudulent actions. The case has been reported to the police for investigation. Case Study 7 *Source: Anti-Money Laundering Bureau, The People's Republic of China (2020)*
Investment Fraud	United States of America	In June 2020, a California man was indicted on fraud charges alleging that he solicited people around the nation to invest in companies that would market pills he claimed would prevent coronavirus infections and produce an injectable cure for those already suffering from COVID-19. The defendant falsely claimed to have developed a cure for the COVID-19 virus and a treatment that prevented a person from being infected by the COVID-19 virus through t text messages, videos, and statements sent to potential investors and posted on the internet. The indictment alleges that he fraudulently solicited investments in two companies with a series of false promises, including miraculous results from the prevention product and the cure, and risk-free and 100 percent guaranteed "enormous returns" on investments. To bolster the claims, the defendant falsely represented that an unnamed party in Dubai had offered to purchase the two companies for USD 10 billion, claiming this offer would secure the victim-investors' investments in the two companies, and that he had secured funding from seven investors who had each already invested between USD 750 000 and USD 1 000 000. The FBI arrested the defendant in March 2020 after he delivered pills – purportedly the treatment that prevents coronavirus infection – to an undercover agent posing as an investor. He has been charged with 11 counts of wire fraud stemming from solicitations he allegedly made to potential investors in Nevada, New York, Texas and Colorado. Two of the charges relate to communications with the undercover agent. Note: In the United States, an indictment contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt. Case Study 6 *Source: Department of Justice, United States of America (2020)*

Type of Case	Jurisdiction(s) Involved	Description
Abuse of Economic Stimulus Measures	United States of America	In July 2020, a tech executive in the state of Washington was charged with one count of wire fraud and one count of money laundering in connection with the alleged submission of at least eight fraudulent Paycheck Protection Program (PPP) loan applications on behalf of six different companies to federally insured financial institutions. The applications sought more than USD 5.5 million in loans. In support of the fraudulent loan applications, the individual allegedly made numerous false and misleading statements about the companies' respective business operations and payroll expenses. The criminal complaint further alleges that he submitted fake and altered documents, including fake federal tax filings and altered incorporation documents. For example, the individual allegedly misrepresented that one of his companies had dozens of employees and paid millions of dollars in wages and payroll taxes. The company, purchased on the internet in May 2020, actually had no employees and no business activity at the time of the purchase. The individual also allegedly transferred at least USD 231 000 in fraudulently obtained loan proceeds to his personal brokerage account for his personal benefit. This case was investigated by the Federal Housing Finance Agency's Office of Inspector General, the Internal Revenue Service-Criminal Investigation, the U.S. Treasury Inspector General for Tax Administration, and the Federal Deposit Insurance Corporation's Office of Inspector General. Note: In the United States, a criminal complaint is merely an allegation and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. Case Study 8 *Source: Department of Justice, United States of America (2020)*
Abuse of Economic Stimulus Measures	United States of America	As part of an investigation by the Organized Crime Drug Enforcement Task Force (OCDETF) targeting high-level heroin and methamphetamine traffickers in South Carolina, agents learned that some of the drug trafficking targets were also engaged in wire fraud and money laundering. In September 2020, seven individuals were charged in an indictment with laundering over USD 750 000 in fraudulently obtained funds, including over USD 390 000 from a Paycheck Protection Program (PPP) loan. According to court documents, one of the individuals submitted a fraudulent PPP loan application, along with fraudulent supporting documents that made numerous false and misleading statements about the company's number of employees and payroll expenses. The individual allegedly received a loan of more than USD 395 000, which he disseminated to other members of the conspiracy through various means. Shortly after, he made three bank withdrawals totaling nearly USD 350 000. During recorded calls, another individual informed a third that the scheme involved fraudulent bank applications and that they needed to submit as many applications to the bank as possible by 30 June 2020. Note: The charges in these cases are only accusations of a crime, and defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. *Source: Department of Justice, United States of America (2020)*
Abuse of Economic Stimulus Measures	United States of America	In August 2020, Tarik Jaafar pleaded guilty to defrauding the Paycheck Protection Program (PPP). According to court documents, Jaafar conspired with his wife to create four shell companies, which conducted no legitimate business and existed solely as a means to execute the scheme to defraud. Between April 13, 2020 and May 6, 2020, the couple applied for 18 separate PPP loans in the names of the four shell companies valued at approximately USD 6.6 million, falsely claiming, among other things, that the businesses had employees and they needed the loans to pay their employees' salaries. The couple fraudulently induced banks to distribute approximately USD 1.4 million in loans, which they intended to use for their personal benefit. On June 20 2020, the couple was arrested at a New York City airport as they attempted to flee to Poland. The majority of the funds were recovered by the banks and by law enforcement. Tarik Jaafar pleaded guilty to conspiracy to defraud the United States, and faces a maximum penalty of five years in prison. The investigation was conducted by the FBI Washington Field Office's Financial Institution Fraud squad and the Small Business Administration Office of Inspector General. *Source: Department of Justice, United States of America (2020)*

Type of Case	Jurisdiction(s) Involved	Description
Abuse of Economic Stimulus Measures	Switzerland	In mid-June 2020, a financial institution granted a COVID-19-loan of around CHF 90 000 (EUR 98 500) to a company active in the construction sector. A few days later, the financial institution was informed that the same company sought an additional loan from another financial institution. In the meantime, most of the original loan was withdrawn in cash or spent for daily consumption expenses. The financial institution therefore filed a suspicious activity report and provided it to the Swiss FIU. The case has been forwarded to the competent Swiss law enforcement authorities where criminal proceedings are currently ongoing. Case Study 9 *Source: Federal Department of Finance. Switzerland (2020)*
Abuse of Economic Stimulus Measures	Italy	Investigations ending in July 2020 revealed that members of a criminal group, linked to a mafia-style organised crime group ("*ndrangheta*"), were running a business purportedly involved in the trading of metals in Italy. However, the business was in fact dedicated to the commission of a number of predicate offences involving COVID-19. The predicate offences involved producing false or misleading tax statements, which were used to fraudulently obtain VAT refunds. The funds were then laundered using banks and the money or value transfer systems. Part of the money was sent to a company located in a foreign country in Europe, another part was sent to a foreign country overseas and the criminals received the correspondent amount in cash in Italy. The VAT fraud generated a false turnover for companies involved into this scheme. In the context of the COVID-19 pandemic, it created the requisite to get public non-repayable grants. The criminal scheme was also used to attempt to request additional economic support. Further investigations revealed that the main suspect used the false turnover generated by the VAT fraud to falsely justify losses due to the pandemic, in order to receive non-repayable grants awarded as COVID-19 countermeasures for three companies included in the criminal scheme. Investigations also detected the criminal attempted to benefit from state-granted loans in the context of measures aimed at supporting the economic system following the COVID-19 emergency. Law enforcement authorities seized nearly EUR 7.5 million worth of assets and financial resources and executed 10 arrests. Case Study 10 *Source: Guardia di Finanza, July (2020*)
Abuse of Economic Stimulus Measures	Spain	In April 2020, the Spanish National Police dismantled a criminal organization that tried to obtain public subsidies for companies and employees affected by the economic crisis of COVID-19 pandemic by generating and using false documents. Members of the criminal organization had in the previous years incorporated around 50 companies with no employees and no activity or turnover. The organization generated and used false documents with the aim of obtaining tax benefits as well as subsidies from the social security system and other public stimulus measures under the name of fictitious employees of those companies. Some members of the criminal group were, before the COVID-19 economic stimulus measures, focused on producing and selling false work contracts for foreign nationals in order to obtain subsidies for them. During the operation, the members of the organization were arrested, a large amount of documents was seized as well as approximately EUR 15 000 in cash, and no stimulus measures were provided to them by the administration. *Source: Financial Intelligence Unit, Spain (2020)*
Abuse of Economic Stimulus Measures	Denmark	In October 2020, the Danish High Court ruled its' first sentence in relation to economic fraud with the COVID-19 relief packages. In this case a 29-year-old man was sentenced to 2 years and 3 months imprisonment as well as a claim of approximately DKK 1.3 million (EUR 170 000) for trying to obtain unjustified compensation for false employments in his company. The total compensation applied for was DKK 427 500 (EUR 57 500). The Danish Business Authority conducted a thorough investigation of the application. As a result, the funds were never granted and the company was reported to the Danish Police. *Source: The Danish Business Authority (2020)*

Type of Case	Jurisdiction(s) Involved	Description
Unemployment Insurance Fraud	United States of America	In October 2020, four individuals in Florida were arrested in a wide-ranging, ongoing joint federal and state investigation into a significant number of fraudulent unemployment insurance claims submitted to the Rhode Island Department of Labor and Training (RIDLT), and elsewhere, for benefits funded in part by the Coronavirus Aid, Relief, and Economic Security (CARES) Act. At the time of the arrests, court-authorized searches resulted in the seizure of more than USD 1.2 million dollars in cash, several hundred debit cards in the names of individuals whose identities were allegedly stolen, a large collection of high-end jewellery, and six firearms. According to court documents, the four individuals arrested, and a fifth defendant, were allegedly involved in complex schemes to use stolen personal identifying information belonging to residents of Rhode Island, and others. They used this information to apply online for unemployment benefits, and to have those benefits direct deposited into one of many bank accounts opened expressly for receiving fraudulently obtained unemployment insurance benefit payments, as well as fraudulently obtained federal and state tax refunds. It is alleged that, using stolen personal identifying information, at least three of the individuals filed fraudulent applications with state unemployment systems to obtain unemployment benefits. The five individuals are all alleged to have withdrawn fraudulently obtained funds shortly after the funds were deposited and posted to bank accounts in the names of other individuals. This ongoing investigation is being conducted by the United States Attorney's Office, Rhode Island Department of the Attorney General, Federal Bureau of Investigation, Rhode Island State Police, Internal Revenue Service Criminal Investigations, and the Department of Labor – Office of Inspector General. Note: The charges in this case are only accusations of a crime, and defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. *Source: Department of Justice, United States (2020)*
Misappropriation of Government Funds	Russia	An audit revealed that a private enterprise contracted out by the State body was purchasing medical equipment at significantly inflated prices for a total amount of over RUB 3.1 billion (EUR 35 million). With the help of the Russian FIU materials, a criminal case (on the grounds of fraud in organized group) has been initiated against officials of the enterprise for the embezzlement of budget funds in the amount of RUB 27 million (EUR 300 000). These funds, a part of the total sum of the contract, have been cashed out. Information about the identified suspicious financial transactions and the schemes of financial connections of the persons involved were sent to the LEAs and cooperation with a foreign FIU continues. *Source: Rosfinmonitoring (2020)*
Misappropriation of Aid	Tunisia	In October 2020, the financial intelligence unit of Tunisia (CTAF) received a suspicious transaction report from a financial institution indicating that a Tunisian citizen (Mr. X) cashed in a TND 2 million bank cheque (approx. USD 724 000) into the account of his firm, Company C. Mr. X claimed that the consulate of a foreign country issued the cheque to him. It allegedly intended to provide 2 000 foreign citizens stranded in Tunisia during the containment period with accommodation, medicines, supplies and COVID-19 tests. On the same day that Mr. X cashed the cheque, he transferred the entire amount to different accounts held by natural persons, clinics and his brother's firm, Company A. Shortly after, the CTAF received another suspicious transaction report from a different financial institution, which was triggered by the fact that the account of Company A received five identical wire transfers from Company C on the same day totalling TND 400 000 (USD 145 000). Further analysis showed that within a short time span (less than 6 months after opening the account) Company C received six wire transfers only from the mentioned consulate for a total amount of almost TND 7 Million (USD 2.5 Million). Shortly after, TND 500 000 (USD 182 000) were withdrawn in cash, TND 2.5 million (USD 910 000) were transferred to Company B's account (owned by Mr. X), and TND 700 000 (USD 255 000) were transferred to Mr. X's personal account.

Type of Case	Jurisdiction(s) Involved	Description
		Mr. X spent only 15% of the sum received from the foreign consulate on hotels, clinics and pharmacies. The contract between the consulate and Company C, did not define the services required from the company, the prices, or the taxes involved. Further, Company C has no other bank accounts or economic activity. Meanwhile, transfers sent to Company A were found to be based on fraudulent invoices, containing abnormally high prices compared to those normally charged. Consequently, CTAF concluded that Mr. X used a shell company (Company C), family companies and fraudulent invoices to misdirect public aid given by a foreign country to its citizens stranded in Tunisia because of the COVID-19 pandemic The CTAF ordered, as a preventive measure, a freezing of the accounts of companies A, B and C, and Mr. X's bank account. The CTAF sent a spontaneous disclosure to the foreign financial intelligence unit and transmitted the report to the prosecutor. The investigation is ongoing. Case Study 11 *Source: Financial Intelligence Unit, Tunisia (2020)*
Corruption - Fraud Involving Government Supply Contracts	Italy	In April 2020, a large Italian company in the garment industry obtained a public contract of around EUR 1.5 million for the supply of gowns and other personal protective equipment. This company was managed and owned (through a fiduciary mandate) by a close relative of the contracting authority's president, who qualified as a politically exposed person (PEP). The company obtained the procurement contract by a direct assignment, without a tender procedure. A month later, a financial institution informed the Italian FIU of an outgoing bank transfer of EUR 750.000 from a bank account held abroad by the PEP through a fiduciary mandate to the awarded company. Such funds, in turn, originated from previous transfers involving foreign opaque legal entities in particular trusts and foundations, allegedly linked to the same PEP and based in tax havens. In the meantime, the supply was converted into a donation, apparently after the hints of investigations into the matter, and some credit notes were issued by the awarder company in order to call off the original invoice, which would have been issued (as declared by the parties) by mistake. The Public Prosecutor's Office opened a knowledge dossier initially without suspects or hypotheses of crime. Then, the same Prosecutor started a criminal proceeding for bid rigging and fraud involving public supplies. Proceedings are currently ongoing before the Court. *Source: Financial Intelligence Unit, Italy (2020*)
Corruption - Fraud Involving Government Supply Contracts	Russia	*During the course of mandatory inspection, suspicious financial transactions with the participation of persons involved in the audit were identified. The case is associated with a possible overpricing of medical masks. Company A is suspected to have accepted and issued invoices with VAT included on products which were not subject to VAT. The three buyers involved in the suspicious transactions came from both private companies and public entities and had paid a total of RUB 115 312 714 (EUR 1 270 000) for the overpriced masks.* *This is considered an unjustified overprice of goods also supplied to organizations with state participation. Later, part of the funds was withdrawn to the accounts of two companies with the indicators of fictitiousness. The suspicion around those companies was raised in the course of carrying out mandatory due diligence and control measures over operations with funds and other property, carried out by Rosfinmonitoring employees. The activities performed matched a list of indicators of fraudulent transactions, which is why the findings of the inspection have been forwarded to LEAs and await further action.* *Source: Rosfinmonitoring (2020)*
Abuse of Remote Working Conditions	Ethiopia	A bank employee illegally withdrew ETB 3 million (EUR 68 300) from an inactive customer account and lent it to his friend without any collateral. When the internal auditors of the bank discovered the illegal withdrawal of money from the inactive account, they reported the case to the Ethiopian Financial Intelligence Centre as a suspicious transaction. The Centre then conducted analysis and sent the results to law enforcement authorities for further criminal investigation. Both the bank employee and the individual who received the money are under investigation. They have been charged with corruption and other related financial crimes and temporarily released from custody on bail. The case is still active.

Type of Case	Jurisdiction(s) Involved	Description
		This offence occurred during a state of emergency declared in Ethiopia to contain COVID-19. Due to the measure, only 50% of employees were working in the bank while the rest were working from home. This allowed the employee to exploit the system and commit the crime. In addition, many businesses were continuously inactive during the state of emergency. Both scenarios created vulnerabilities. Further, the control systems in financial institutions were weaker due to the reduction in the number of employees physically present at the banks to perform know-your-customer, customer due diligence measures, etc. Note: The charges in these cases are only accusations of a crime, and defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. Case Study 12 *Source: Ethiopian Financial Intelligence Center (2020)*
Virtual Assets	Hong Kong, China	Between late February and early March 2020, an owner of a health-care products trading company in Hong Kong, China saw internet advertisements posted by several purported sellers of surgical masks and medical equipment, including on a major social media platform. When she attempted to purchase the equipment, she was deceived into transferring HKD 450 000 (USD 58 000) to various bank accounts in Hong Kong, China and an Eastern European country and into converting the equivalent of HKD 3.96 million (USD 510 000) into Bitcoin. To do so, the victim withdrew cash from her personal bank account and deposited the cash to a designated Bitcoin ATM where the funds were transferred to designated Bitcoin accounts. In total, three banks located in two jurisdictions (Hong Kong, China and an Eastern European jurisdiction) were involved. Five transfers ranging from USD 47 250 to USD 235 830 worth of Bitcoins were transferred to accounts owned by the culprit. All of the scammers stopped responding to the victims after receiving the payment. The investigation is ongoing. Case Study 13 *Source: Financial Services and the Treasury Bureau, Hong Kong, China (2020)*

FATF

www.fatf-gafi.org

December 2020