Criminal activities bloomed during the COVID-19 pandemic

During these unprecedented times of the COVID-19 pandemic, criminals around the world are taking advantage of the situation and are finding new ways to generate illicit funds by adapting their modus operandi or developing new criminal activities.

Money Laundering and Terrorism Financing (ML/TF) threats have emerged following the advent of COVID-19. Indicatively, some of those risks are listed below:

Cybercrime - Social distancing restrictions has increased cyber security risks for users because of the increased demand for online information and supplies. Through phishing emails, for example, criminals have attempted to use the World Health Organization brand to obtain personal information from unsuspected individuals. Several cyber-attacks have also taken place against organisations and individuals (e.g. malware via malicious links and attachments). According to Europol, law enforcement partners have also reported an increase in "online activity by those seeking child abuse material" as "offenders welcome opportunities to engage with children whom they expect to be more vulnerable due to isolation, less supervision and greater online exposure". Where such services are accessed via cryptocurrency payments, this may present a ML/TF threat for Virtual Asset Service Providers (VASPs).

Fraud - Well-known fraud techniques have been employed by fraudsters to target individuals and organisations during this pandemic. For example, criminals make calls to victims impersonating either a clinic or a hospital official, claiming that a relative of the victim has fallen sick with the virus and request payments for medical treatment. Another example is the fake medical and protective equipment being marketed as protection against the coronavirus and scams relating to internet banking accounts, such as 'phishing' emails connected to COVID-19 that appear to be from the bank and that may be related to financial support available in the wake of the pandemic, but which are actually a lure asking the individual to provide or validate their account or identity information. Action Fraud UK, recently reported a 400% increase in coronavirus-related frauds for March 2020.

Bribery and corruption related to government support schemes - Incentive packages have been issued by governments to support businesses throughout the economic recession caused by COVID-19. A potential opportunity for misuse by those who administer them might be born. Tax benefits, advance payments, funded public loans, state guarantees for loans taken from banks, funded protective equipment, are some of the measures that may create an opportunity for abuse and corruption. An event that recently grabbed the headlines in Cyprus, was the arrest of two individuals for the alleged sale of masks provided for free by the Republic of Cyprus to semi-governmental and public organisations. Closure of handling facilities such as ports and airports used for international commerce, creates an opportunity for bribes paid to customs and other officials.

Trafficking in counterfeit medicines and other supplies - This includes the distribution of fake products for which the demand has increased rapidly during the pandemic. An example is the distribution of fake COVID - 19 testing kits. A team of agents from Homeland Security Investigations in the US, found the fake COVID-19 treatment capsules and tests at the Port of Baltimore, hidden in boxes under packets of Chinese tea.

Robbery or theft - Organised crime groups have taken advantage of the pandemic to increase crimes related to thefts, burglaries, robberies, and other criminal activities. Elderly could be an "easy" target for criminals as they are potentially more vulnerable to exploitation. In this respect, if the perpetrator approaches the elderly victim at home by pretending to be a law enforcement officer or a healthcare official offering testing for COVID-19, could steal valuables easily.

Insider trading and market manipulation - Having a significant number of employees working remotely might have caused a possible leak in secure communication channels, has given rise to the risk of market abuse due to a potential leakage of confidential information.

In addition, industries such as pharmaceuticals, are likely to be more vulnerable to the threat of market abuse. For instance, the pharmaceutical sector has reacted with large price swings in share prices due to their involvement in studying the development of VOVID-19 vaccine.

Now more than ever, organisations are called upon to enhance their existing system of internal controls in order to minimise, to the extent possible, such events from happening. This is the right time for organisations to introduce or enhance their Policies and Procedures, such as Anti-Money Laundering and Terrorist Financing, Anti-Bribery and Corruption and Whistle Blowing. Likewise, monitoring and control processes should be aligned with new threats and emerging risks in order to be effective in identifying and reporting attempts to commit criminal offences.