Fight against money laundering in face of COVID-19 (2/17/20)

In times of adverse and significant events, such as a war, crisis or pandemic, there is a certain group of people that will try to exploit the national emergency situation in their own interests. It is no surprise that this phenomenon has now surfaced in response to the global outbreak of COVID-19. At the very outset of the pandemic, cybersecurity companies and news agencies repeatedly warned us about an increase in phishing attacks, with people receiving virus reports from authorities such as the WHO enticing them to download malware on their devices.

Professionals being responsible for compliance with financial rules recognise that risks associated with COVID-19 go beyond the old fraudulent activities and schemes. With risk levels growing and their profiles changing significantly, many organisations that lack prudent risk management might find themselves overloaded or insufficiently trained.

No statistics are currently available on how the pandemic is affecting processes involved in money laundering, and the precise outcome is not to be seen until a later date (e.g. judging from the number of reports on suspicious transactions sent by the banks). We can so far draw only theoretical conclusions and try to predict exploitative methods of money laundering.

There are a number of aspects capable of affecting AML:

1. As a result of the pandemic, many banks asked their customers to stay away from their branches and to try and make payments and other transactions using innovative banking products mainly characterised by remote usage. Such products are always viewed as high-risk services compared to the customer's physical presence at the bank and direct contact with the bank staff.
2. Some services, such as opening an account, are not commonly offered without the customer's physical presence. This service has now become more flexible as a result of rapidly falling customer numbers. In this case the banks are having to strengthen their safeguards and risk procedures (e.g. digital identification and biometric recognition of customers).
3. The number and quality of reports on suspicious transactions or suspicious activities might be affected by the fact that the staff of many financial institutions are working remotely. One reason is that those workers might not have full access to the databases they are using for customer checks (e.g. only one officer has access).
4. As many people are out of work and stuck abroad (students or workers), they might be receiving monetary support from their family abroad, something their bank's financial system can flag as "unusual behaviour" causing the bank to take extra measures for risk mitigation.
5. Attention should be paid to an increase in cash withdrawals as many companies might be evading taxes by hiding their real transactions, for example, to demonstrate diminished profitability and qualify for state aid.
6. Companies might be trying to cut their labour costs by paying royalties instead of salaries. A rapid increase in such payments compared to fixed salaries may suggest tax evasion if royalty agreements are considered uncharacteristic of this trader or recipient of royalties.
7. Since the beginning of the year we have observed an increase in some types of money laundering activities, such as money mules being hired online through various social networks. A money mule is someone who receives money in their bank account from a third party and then transfers the money

into a different account, or withdraws cash and passes it to someone else in exchange for commission. With people losing their jobs or being forced to look for home working options, the chance to make a quick buck by transferring money from one account to another may seem very attractive. However, the number of cash operations has dropped considerably in countries that are hard hit by COVID-19. International terrorist groups have scaled down their activities in Western countries because COVID-19 outbreaks may affect terrorism financing streams.

What can we do today?

Below we recommend some ways to fight against financial crime risks during the pandemic given the huge uncertainty inherent in this situation:

1. Revise your internal system of AML controls and assess risks! Which risk is more global in the face of COVID-19? Which controls can be reduced? You need to update your scenarios of suspicious transactions based on typologies prevalent in times of global crisis.
2. Check your internal risk procedures to make sure you have reliable protocols in place for dealing with a breach!
3. Assess whether your risk management function is capable of providing the same level of protection in the present situation! If you need more expertise, engage independent consultants who can help you remotely and offer some fresh perspectives.
4. Keep adapting to the emergency situation and add the potential economic crisis to your list of events!
5. Increase the involvement of your staff in the fight against financial crimes through distance learning!