# FIAU Guidance Note

## COVID-19: REMAINING VIGILANT AGAINST A CHANGING CRIMINAL LANDSCAPE

FIAU
MALTA
FINANCIAL INTELLIGENCE ANALYSIS UNIT

## The FIAU understands that subject persons are facing unprecedented challenges and operating in difficult circumstances brought about by the COVID-19 pandemic.

It has now become clear that the virus is a breeding ground for criminals and criminal organizations seeking to exploit the situation. The ensuing economic crisis has likewise given criminals the opportunity to thrive. As Europe starts to gradually emerge from the holds of the pandemic, the criminal landscape begins to flourish, and the risks of money laundering and terrorism financing are only starting to increase.

As part of its ongoing assessment of the situation, the FIAU would like to advise on current and anticipated threats, address arising concerns, and remind subject persons to remain vigilant in the face of ML/FT risks.

# The criminal impact of the covid-19 pandemic

International law enforcement agencies and other bodies are in constant communication with authorities to understand the types of illicit behaviour detected across the world during this period. This information is disseminated across authorities and regularly published in the form of publicly available reports. The FIAU is also in possession of information and data on current criminal trends.

## Information clearly indicates an increase in specific types of illicit behaviour, but also an emergence of new activities related to the pandemic. Across Europe, these trends are being noted:

- **FRAUDULENT SALE OF MEDICAL PRODUCTS:** An increase in fraud relating to the marketing and sale of pharmaceutical and healthcare products, either through non-delivery of goods for which payment has been made in advance, or the delivery of counterfeit, substandard or defective goods;
- **BENEFIT AND COMPENSATION SCHEME FRAUD:** Fraudulent applications for compensation schemes intended to assist businesses and employers, with criminal organizations applying under the guise of an existing company, but providing their own bank account details.
- **CYBER-ATTACKS:** An increase in cyber-attacks on online users, including phishing campaigns to obtain confidential data such as bank and credit card details, as well as ransomware attacks to elicit payment from victims. Ransomware attacks are more pronounced among higher risk sectors (hospitals, delivery and transportation systems). Locally, a surge in CEO fraud and business email comprise cases has been noted;
- **PAYMENT FRAUD:** An increase in criminal activity connected with payment fraud and fraudulent investment opportunities;
- **EXPLOITATION MATERIAL:** An increase in the search and production of child sexual exploitation material online (including on the dark web);
- **TRADE IN ILLEGAL GOODS:** An increase in the online trade of other illegal goods and services through the dark web.

# The changing circumstances brought about by the pandemic and the ensuing economic crisis will continue to shape criminal activity in both the short and mid-term, but also in the years to come:

- **Cash intensive businesses** that were previously misused to launder dirty money have slowed down or halted their economic activity. This has restricted the channels used for money laundering, resulting in large volumes of cash waiting to be laundered. There are concerns that small to medium businesses, particularly those on the brink of bankruptcy, will be highly vulnerable to abuse by criminal organisations, as these swoop in to "invest" in failing businesses and simultaneously launder their cash.

- Persons who have been hard-hit by job losses and slow business are easy targets for **recruitment by both criminal and terrorist organizations**, with the promise that the financial and medical needs of their families will be taken care of.

- The **real estate sector** continues to be attractive to criminals, as they attempt to launder funds by purchasing real property in cash (bank notes).

- The launch of public aid schemes to revitalize the economy may give rise to an increase in **corruption**, by those seeking to siphon these newly available government funds into their personal pockets.

**Criminals have clearly taken advantage of the global pandemic itself, but are also preparing to exploit the long-term effects of the economic crisis. Subject persons are advised to stay up-to-date on the latest trends by referring to reports published by reputable international bodies, including but not limited to EUROPOL, the FATF, INTERPOL and the UNODC.**

# MITIGATING MONEY LAUNDERING RISKS

As criminals seek to receive and launder funds through the financial system, the FIAU urges all subject persons to remain vigilant and ensure that their procedures are fully aligned with the latest Prevention of Money Laundering and Funding of Terrorism Regulations and the FIAU Implementing Procedures.

Special attention should be paid to particular aspects of the AML/CFT regime:

## Revising the Business Risk Assessment

Subject persons are to consider whether and to what extent their products and services may be misused or exploited by criminals and money launderers, particularly in light of threats highlighted earlier in the document. The Business Risk Assessment is a dynamic tool which must evolve in response to changes, including external changes. The current circumstances may indeed require an evaluation and revision. Please refer to Section 3.3.4 of the FIAU Implementing Procedures Part I for guidance.

## Updating the Customer Risk Assessment

Public health restrictions have led to low or very limited activity within certain economic sectors. On the one hand, subject persons should be mindful of high value transaction flows through businesses which should, in the current circumstances, be experiencing low or no business activity. This may indicate that the entity is being used as a front to channel and layer illicit proceeds. On the other hand, many businesses have adapted to these restrictions by changing the way they offer their products and services. Where a significant departure from the known risk profile is noted, subject persons should request additional information and documentation to justify changes in activity. On the basis of an assessment of such information, subject persons are to consider whether to revise and update existing Customer Risk Assessments.

Please refer to Section 3.5 and Section 4.5.2.2 of the FIAU Implementing Procedures Part I.

## The FIAU would also like to remind subject persons to:

- Onboard customers in full compliance with AML/CFT regulations and procedures at all times, ensuring that due diligence measures are commensurate with the level and nature of risk posed;
- Carry out appropriate ongoing monitoring to be in a position to detect suspicious transactions;
- Continue providing employees with all the necessary resources and training to carry out their compliance duties to the fullest;
- Assess transactions and activity for red flags and immediately report suspicious transactions to the FIAU.

# REMOTE ONBOARDING PROCEDURES

The global pandemic has evidently shifted the way business is carried out, with more subject persons now working away from their physical offices and branches. Essential social distancing efforts have restricted the amount of contact with clients, and disruptions in postal and courier services may have likewise had an impact on identification and verification procedures.

Subject persons should now, more than ever, seek the guidance of the FIAU Implementing Procedures Part I to tailor their established policies and procedures to ensure that they can continue carrying on business while fulfilling their regulatory obligations. Entities who have accelerated the digital transformation of their businesses should test and assess their systems to ensure that all anti-money laundering obligations can be fully adhered at all times.

When it comes to verifying the identity of customers, the FIAU Implementing Procedures permit the use of digital copies or scans of documents in lower risk scenarios, without the need to carry out additional measures. In other cases, subject persons are to consider applying one or more of the additional verification measures listed in Section 4.3.1.2, which may all be carried out remotely. These include, among others:

- Requesting additional identification documents, to verify the same information through different sources;
- The use of video conferencing tools, identity verification software or platforms, or e-IDs;
- The use of commercial electronic data providers;
- Ensuring that the first transaction into the account is carried out through another account held by the same customer with a credit or financial institution set up in a reputable jurisdiction, or by transferring a small amount of funds to a bank account held by the customer and asking them to return the funds;
- Holding a welcome call with the customer via a verified telephone number to confirm certain personal information.

These measures are not exhaustive, and subject persons can apply other methods and checks as long as they are adequate and assist in determining whether the customer really exists and that they are who they purport to be.

Finally, subject persons are encouraged to take advantage of non-face-to-face verification measures to protect the health of their employees and customers and of the public at large.

Utilized to their fullest, the FIAU Implementing Procedures provide the flexibility needed to adapt to changes in circumstances while remaining effective in the fight against money laundering and funding of terrorism.

**The FIAU remains available to assist subject persons. Questions on the application of AML/CFT measures may be sent to queries@fiumalta.org**