MONEYVAL: Money Laundering and Terrorism Financing Trends during the COVID-19 Crisis

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

András Csúri

AUTHOR

András Csúri

Vienna University of Economics and Business

Published in
2020, Vol. 15(3) eucrim pp 197 – 198

ISSN: 1862-6947

https://eucrim.eu

On 2 September 2020, MONEYVAL published a report outlining general assumptions and preliminary conclusions on threats, vulnerabilities, and best practices identified during the ongoing corona pandemic. The report is based on information received from its members. It aims to assist policy-makers, practitioners, and the private sector in applying a more targeted and effective response to emerging ML/TF risks.

The report underlines that criminals have updated their *modus operandi* to gain additional profits by exploiting the upheaval generated by the COVID-19 pandemic. While the level of criminality remained stable, there has been a surge in certain crimes, especially those with transnational elements, e.g., fraud through electronic means, the sale of counterfeit medicines, and cybercrime.

The promptly implemented economic and relief measures aiming to support businesses and individuals have created new opportunities for misappropriation. Furthermore, the urgent need to acquire specific medical equipment and supplies in some countries has led to a temporary suspension of complex controls in public procurement procedures, creating vulnerabilities for fraud, corruption, and subsequent ML.

The limits imposed on physical meetings in the private sector have raised supervisors' concerns with regard to the full application of customer due diligence measures. The reporting of suspicious transactions has remained steady. As supervisory control of ML/TF threats shifted to off-site and desk-based reviews, the authorities in charge have found innovative ways to carry out their tasks by using secure electronic means and shared-screen facilities. Domestic information exchange was only minimally disrupted, and international cooperation in the fight against ML/TF does not appear to have been negatively impacted by the measures against COVID-19.

Some of the findings in the report are also relevant for the general public, in particular information on potential criminal schemes, such as phishing emails, text messages containing links to malicious websites, attachments with the aim of obtaining personal payment information, and social engineering.

Based on these findings, the report offers a number of recommendations in all the above areas, *inter alia*:

- Any exemptions or simplified measures should be properly justified and supported by a risk analysis;
- Jurisdictions should continue to provide assistance to the private sector by communicating relevant information on risk situations, including the present report;

- Authoritires should closely monitor the situation of public procurement, especially where controls have been relaxed;
- More resources should be placed into off-site monitoring when on-site controls are not possible;
- Jurisdictions should be able to provide to foreign counterparts all relevant information on legal persons to the fullest extent possible, as criminals are actively using foreign legal persons to commit fraud offences.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union