Financial Intelligence Authority

Rwenzori Towers (Wing B) 4th Floor, Plot 6, Nakasero Road Kampala, Uganda
P.O. Box 9853, Kampala Tel: +256 417 892 600 E-Mail: fia@fia.go.ug

STATEMENT BY THE FINANCIAL INTELLIGENCE AUTHORITY: CONCERNS RELATED TO THE CORONAVIRUS DISEASE 2019 (COVID-19) AND MEASURES TO COMBAT INCREASED MONEY LAUNDERING/TERRORIST FINANCING ACTIVITY

The FIA requests financial institutions and other reporting entities under the Anti-Money Laundering Act affected by the COVID-19 pandemic to contact the FIA as soon as practicable if the institution has concerns about any potential delays in its ability to file the required large cash transaction (LCTR) and suspicious transaction reports (STR). The institutions seeking to contact the Authority should call **041 789 2600** or e-mail at **fia@fia.go.ug.** The FIA will continue to be available to support such institutions for the duration of the COVID-19 pandemic.

With people facing confinement or strict social distancing measures, in-person banking and access to other financial services is difficult, and unnecessarily exposes people to the risk of infection. The FIA encourages the fullest use of responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures put in place by the Government of Uganda. While unintended, these measures may provide new opportunities for criminals and terrorists to generate and launder illicit proceeds.

The FIA advises financial institutions to remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters. We are monitoring public reports of potential illicit behavior connected to COVID-19 and note the following emerging trends:

1. **Increased Fraud:** Reports consistently indicate that criminals have attempted to profit from the pandemic through fraudulent fundraising for fake charities, various medical scams (including investment fraud) and online sales of counterfeit medicines and medical supplies, such as testing kits and personal protective equipment.

2. **Cyber Crime:** Criminals exploit concerns about COVID-19 to insert malware on personal computers or mobile devices. In recent phishing attempts, criminals created fake World Health Organisation emails, embedded malware in mobile applications for tracking COVID-19 cases, and sent malware via text messages claiming to be healthcare providers requesting payment for treatment or promising to provide emergency relief funds.

3. **Changing financial behaviours:** There is an upward trend in remote transactions as financial institutions close branches and offices or operate on reduced hours. Customers unfamiliar with online platforms may be more vulnerable to fraud and those without access to online financing options may move assets to the informal economy.

4. **Financial Sector Volatility:** In an economic downturn, criminals and terrorists may seek to invest in real estate or troubled businesses, which can be used to generate cash and mask illicit proceeds, or use corporate insolvency proceedings to mask funds' origins. Illicit proceeds can also be introduced to the system as customers look for new ways to restructure loans and lines of credit. There is also a concern that large withdrawals of cash, and liquidation of share portfolios may provide an opportunity for money launderers to mingle illicit funds with clean money when funds are later put back into the system.

5. **Terrorist Financing:** Increased concerns about terrorist groups using the COVID-19 crisis to raise or move funds, including by increasing their illicit activities to raise funds.

6. Increased use of online schemes and/or virtual assets as a layering method to launder proceeds;

7. Criminals finding ways to exploit temporary issues in internal controls caused by remote working situations to bypass Customer Due Diligence measures;

8. Potential increases in transactions not in line with customers' profiles, the use of the informal economy to provide financing as traditional gatekeepers are locked down, and increases in bulk-cash movements;

Financial institutions and other businesses should remain vigilant to emerging money laundering and terrorism financing risks and ensure that they continue to effectively mitigate these risks and are able to detect and report suspicious activity.

The FIA is ready to provide further AML/CFT guidance to support the current national efforts to tackle the COVID19 crisis and its effects, and welcomes feedback.

Thank you for your continued support.

Sincerely,
Sydney Asubo
Executive Director

Vision: To be a Centre Of Excellence In Combating Money Laundering And Terrorism Financing.