How COVID-19 has impacted the Money Laundering (ML) and Terrorist Financing (TF) Environment

We are currently facing a COVID-19 pandemic which has undoubtedly led to global challenges, human suffering and economic disruption. This unprecedented pandemic has created a new normalcy in business operations and practises, consumer behaviour, regulations, trades and policy enacted in parliament. Criminals are taking advantage of the chaos and uncertain environment to conduct their illegal activities. Research has shown an increase in new money laundering and terrorist financing threats and vulnerabilities as fraudsters improve their craft in this trying period.

The Financial Action Task Force (FATF) published a paper in May 2020 regarding the above to urge Financial Institutions (FIs) to remain vigilant of the emerging threats and vulnerabilities.

New Threats and Risk Emerging from COVID-19-Related Crime

Fraud

Criminals have increased their fraudulent activities and attempted to profit from the COVID-19 pandemic. Some of the criminal's modus operandi include impersonation of government officials, online purchase scams, production of counterfeit essential goods and fundraising for fake charities.

Money Laundering

Governments around the world in dealing with the COVID-19 pandemic have rolled out various support schemes, travel restrictions, restricted movement measures and relief initiatives to support the economy and slow down the spread of the virus. These measures inadvertently have opened up new avenues for criminals and terrorists to launder their illicit proceeds.

Citizens in many areas of the world are being told by health or political authority to remain in their homes to help halt the spread of COVID-19. These measures have caused online transactions to spike due to the change in consumer behaviour.

A shift in the consumer patterns, business operations and a disruption in global supply chains impacted by COVID-19, have resulted in transnational organised crime devising schemes to launder their illicit proceed from illegal activities.

Cyber Crime

There has been a sharp rise in social engineering attacks, phishing email, ransomware, spams and fraudulent websites. Criminals are exploiting the increased concerns for COVID-19 awareness to introduce malware on personal computers and mobile devices.

Telecommuting has increased 10 fold as businesses allow their employees to work from home. Cybercriminals and hackers are also exploiting the sharp rise in global remote connections and weaknesses in the companies' network security to steal valuable customer information.

Other Predicate Crime

Criminals may take advantage of the pandemic to exploit vulnerable groups as there has been an increase in unemployment and reduced activity for detecting of human trafficking by government agencies.

With the closure of schools, demands for online child-related materials amid the lockdown may lead to the exploitation of children in the production and distribution of these products.

Other Money Laundering Vulnerabilities

- Change in Financial Behaviours
- Misdirection of Government Funds
- Increase risks of corruption
- Increase financial violability

Enhancements to FIs Current AML/CFT Policy

AML/CFT regimes impacted as a result from COVID-19 includes the postponement of AML/CFT onsite inspections, the substitution of such inspections with remote inspection and the significant deceleration in AML/CFT matters like technical assistance and formulation of new initiatives, due to the shift in the focus of many FIs.

Other impact involves the delay of issuance of licenses, postponement of certain prosecutions resulting from suspension of trials, increase in vices like online gambling and certain industry shutting down due to migrant workers confinement measures.

Notwithstanding the above, FIs can consider some of these suggestions to further enhance their AML/CFT policy.

- FIs should educate its employees to diligently notify supervisors if they encounter any trouble in the reporting of STRs.
- FIs are encouraged to set up response teams to assess and identify risk, system and resilience on a continuous basis and to develop responses accordingly. These teams should continuously engage with supervisors to ensure sufficient prioritisation measures have been taken.
- FIs are also advised to be flexible in applying CDD measures based on the level of risks identified.
- FIs are encouraged to make use of technology available, including Fintech, Regtech and Suptech to their fullest extent to identify emerging ML and TF risks and to effectively mitigate these risks.

Conclusion

The COVID-19 pandemic has posed many challenges, as well as heightened risks and vulnerabilities. However, FIs are expected to maintain sound risk management and maintain a high level of defense against these threats.

FIs should also remain vigilant to heightened risks such as cybersecurity threats, fraudulent transactions and scams, money laundering, and terrorism financing while managing the COVID-19 pandemic.

FIs are also reminded to seek support, guidance and assistance from authorities and qualified service providers on the relevant laws and regulations that should be applied during the current crisis.

RHT Compliance Solutions

RHT Compliance Solutions is a premier Compliance Service Advisory firm based in Singapore.

Our team comprises experienced and certified professionals with extensive regulatory, compliance and risk management experience from Singapore, Indonesia, Hong Kong and the broader region. The team is well equipped to provide clients with intelligent, risk-focused and cost-effective solutions.

Full text can be found here.

Reach out to us:

Jarvis Lee
Compliance Analyst
jarvis.lee@rhtgoc.com

RHT Compliance Solutions
1 Paya Lebar Link #06-08
PLQ 2 Paya Lebar Quarter
Singapore 408533
cs@rhtgoc.com

Visit us