

ADVISORY ON RISKS ASSOCIATED WITH COVID-19 PANDEMIC

Introduction

The current COVID-19 pandemic across the globe has in no doubt altered the way we do things, most especially with the limitation to public life and lockdown measures put in place by countries to curb the spread of the virus from person to person. These measures have increased the use of digital commerce via the internet as a means to encourage social distancing.

The focus of the three tiers of Government at the present time is on fighting this pandemic. It is however clear that criminals are taking advantage of the COVID-19 crisis to carry out financial fraud and exploitation scams. The intention of this advisory is to support the Government's effort by ensuring that funds meant for the health and safety of the citizenry are not diverted, misappropriated nor exposed to various medical exploitation scams which include malicious or fraudulent cybercrimes.

The advisory highlights and draws the attention of relevant Law Enforcement Agencies (LEAs), Regulatory /Supervisory Authorities including other AML/CFT stakeholder agencies to take necessary precautionary measures to the trends and patterns identified from both financial transaction reports and other information available to the NFIU within this crisis period. The red flag indicators and case studies highlighted herein are to help in the fight against financial crimes and prevent criminals from taking advantage of any vulnerabilities arising from the current situation.

Vulnerabilities, Threats and Emerging Patterns during the COVID-19 Pandemic

A comprehensive analysis of all COVID-19 related Suspicious Transaction Reports (STRs) and other transaction reports available to the NFIU suggests certain vulnerabilities in the financial system most especially related to the healthcare, procurement, public and the Designated Non-Financial Businesses & Professions (DNFBPs) sectors.

It is important to identify the key factors responsible for the observed pattern of crime in the country. They include excess demand for Personal Protective Equipment (PPE) and pharmaceutical products, government-imposed lockdowns which limit access to certain goods and services and the need to **Work from Home (WFH)** to preserve public health. Most activities are now online and with increasing anxiety and uncertainty there is a real danger that criminals will seek to exploit the situation to commit crime and launder proceeds from illegal activities.

1. Cyber crime

The COVID-19 pandemic has given rise to an unprecedented level of attempted internet fraud. Google reports blockage of over 18 million COVID-19 related scam emails every day¹. The most

¹ BBC News report where Google claims to block at least 18 million corona virus scam emails to protect users on its web-based application google chrome which is one of the most widely used browsers. The report was filed on 17th April and can be found on its website through this link: <https://t.co/qkMZUyrl6s?amp=1>

common forms of cybercrime is through social engineering attacks which include: Phishing emails, spam campaigns and Business Email Compromise (BEC). Majority of the workforce work from home and are vulnerable to these attacks. Criminals also target organisations and individuals through malicious links, attachments and fake social media accounts.

2. Fraud

Taking advantage of the anxieties of victims and uncertainty surrounding the economy, criminals have devised various “get-quick-rich schemes” which usually turn out to be scams to lure the unsuspecting public. These are normally in the form of imposter, product and investment scams. Imposter scams usually involves criminals pretending to be from international agencies such as the World Health Organisation (WHO) or host fake websites to mimic international agencies and solicit for funds to fight the spread of COVID-19, spread malware and steal personal information. In product scams criminals supply and distribute substandard or unapproved medical supplies and equipment pertaining to COVID-19. Criminals have also been observed to engage in investment scams through the promise of substantial gains on investments in stocks and other speculative activities such as online forex and commodity trading and several other Ponzi type schemes.

3. Counterfeiting and Substandard goods

It is expected that with the massive demand of medical supplies and equipment, criminals will seek to engage in the production, distribution and sale of substandard, unapproved, reused or fake medical products most especially face masks and alcohol-based hand sanitisers.

4. Diversion of Public Funds due to Corruption




A number of the STRs filed suggest the likelihood of an increase in the diversion of public funds by corrupt public/civil servants. Billions of public funds are usually earmarked for the supply of health supplies and equipment, PPEs to hospitals and medical centres across the country.

5. NGO's




NGO's and other charity organisations may be exploited to move illicit funds from donors. Funds transferred to NGOs can also be utilised to fund terrorist activities if strong AML/CFT measures are not implemented. The current COVID-19 crises will definitely put a lot of pressure on the activities of NGOs and this can easily be exploited by criminals to launder funds usually through unrelated third parties. There is an increasing trend in the use of “money mules” to physically move cash between jurisdictions. These are usually vulnerable people in the society who may be taken advantage of, at times without their knowledge to move illicit funds to organised criminal

gangs or to help fund terrorist activities. **Observed Red Flags include the following:**



Cybercrime

-  *No established connection/relationship between sender and beneficiary.*
-  *Quick conversion of funds to virtual currency to be moved to various destinations without trace.*
-  *Failure of customer to produce documentary evidence for transaction on request.*





Fraud

-  *E-commerce merchant with little or no history or internet presence suddenly receiving multiple payments from un-related 3rd parties.*
-  *Individual suddenly receiving multiple payments from un-related 3rd parties.*
-  *Customer suddenly engaged in the supply or purchase of medical supplies and payment for goods or services associated with a known brand, yet beneficiary is an individual not the company.*




Counterfeiting & substandard goods

-  *Unusual transaction dynamics from customer, expect to see more transactions for medical supplies, equipment and medication.*
-  *Payment for goods or services associated with a known brand, yet beneficiary is an individual not the company.*

Diversion of public funds

-  *Unusual volume of transactions, large and frequent cash withdrawals and deposits.*
-  *Immediate disbursements of deposited funds to multiple accounts.*
-  *Account signatory also a public/civil servant.*
-  *Funds transferred from government account to personal account.*

NGOs

-  *Non-profit organization suddenly receiving donations in favour of covid-19 patients or victims.*
-  *Customer account with little or no activity suddenly receiving funds from one or more un-related 3rd parties only for the funds to be transferred to one or more un-related 3rd parties*
-  *NGOs under the guise of paying COVID-19 victims could actually be paying members of a criminal gang or facilitating terrorism financing.*

Case Studies

- 1. A foreigner working with an International health organisation as a technical officer made several cash deposits in US dollars that were not commensurate with his profile, these deposits were immediately withdrawn from the account and converted to naira.*
- 2. An NGO is involved in healthcare and runs a specialist hospital, however, several cash deposits running into millions of naira were lodged into the account which were also disbursed in cash withdrawals during the same period, indicating that the hospital may be being used as a conduit for money laundering.*
- 3. Government agencies feature in STRs moving huge amount of cash that were received from various local government councils and the funds were withdrawn in cash for disbursement to primary health centres (PHC). The reason given for the huge cash handling is lack of access to financial institutions due to locations of the (PHC), contrary to the limit on cash transactions.*
- 4. An entity received huge amount of money from a state Government agency, for the procurement of health-related equipment, it was discovered that the sole signatory to the company is a director in the ministry of health.*
- 5. Government official receives same day transfers running into several millions of naira from a Covid-19 relief fund into personal account indicating diversion of public funds.*
- 6. Unusual large transaction from a joint multinational regional body/charity organisation making a huge outward transfer up to one million USD to a Covid-19 Relief Fund in one of the ECOWAS member states without documentary evidence to support transfer of funds.*

Guidance on managing the risks associated with the COVID-19 crises

It is important to note that there are elevated risks of ML/TF due to the current COVID-19 pandemic. As highlighted earlier, stronger measures and controls in line with the recommended AML/CFT guidelines need to be put in place by all relevant regulators, LEAs and stakeholders in the country to mitigate ML/TF risks.

1. It remains extremely important for competent authorities, regulatory and supervisory agencies to ensure full compliance of operators to the AML/CFT regulatory requirements to help safeguard the financial system.
2. The NFIU also advises reporting entities and competent authorities to inform their employees about potential cyber threats during this period, especially those WFH. Furthermore, they should devise a protection and response strategy to mitigate the threats of cyber-crime.
3. FATF has advised that onboarding of customers through digital means must be encouraged to protect the public from the spread of COVID-19, this will further ensure that the social distancing practice is maintained.
4. Relevant competent authorities should note the increase in attempts by criminals to defraud unsuspecting victims using techniques such as Ponzi schemes, social engineering and Business Email Compromise (BEC). Reporting entities are strongly advised to remain vigilant and share information with customers particularly those related to fraud including ML/TF risks related to

COVID 19 with more emphasis on the need to protect sensitive banking information such as account and token passwords, PIN and BVN.

5. FATF recommends extra vigilance by relevant authorities with regards to the purchase and supply of essential medical supplies and equipment by off-takers. It is expected that criminals would exploit the excess demand for medical supplies and equipment, most especially PPE and attempt to flood the market with counterfeit goods and supplies.

6. Government is expected to respond to the COVID-19 pandemic by purchasing additional medical supplies such as PPEs and pharmaceutical products. Palliatives in the form of cash transfers and distribution of food items are also being rolled out. However, in line with the provisions of the relevant procurement acts, transparency and accountability must be encouraged at all stages of the procurement process to avoid diversion of public funds.

7. Criminal elements may also attempt to take advantage of the COVID-19 pandemic to move illicit financial flows between jurisdictions through various donors and NGOs. Reporting entities and the relevant stakeholder agencies are advised on conducting satisfactory KYC and enhanced customer due diligence (EDD) for customers and registered NGOs where necessary.

The NFIU is committed to its support in securing the Nigerian Financial System from threats during and after the COVID-19 crises and assures all competent authorities of continuous monitoring of public reports of potential illicit behaviours linked to COVID-19 for quick updates where and when necessary. Competent authorities and particularly reporting entities are advised to make reference to **Suspicion of COVID-19 related illicit activity** in STRs/SARs where any of the above red flags (or similar) form the basis of your filing.