ST. KITTS BRANCH
FinancialServices Regulatory Commission

NewsLetter

May 2020
Issue No. 73

COVID-19 Coronavirus FRAUD, SCAMS & OPPORTUNISTIC THREATS

Coronaviruses belong to a large family of viruses which may cause illness in animals and humans. In humans, several coronaviruses are known to cause respiratory infections ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS) and Severe Acute Respiratory Syndrome (SARS). The most recently discovered coronavirus causes the coronavirus disease, COVID-19. The new virus and disease were unknown before the outbreak began in Wuhan, China, in December 2019. COVID-19 is now a pandemic affecting many countries globally. While this pandemic threatens to debilitate the global financial sector, new risks and vulnerabilities stemming from COVID-19 related crimes have surfaced. It is therefore important for Governments and Regulatory Authorities to assess the impact of COVID-19 on the country's Anti Money Laundering/ Countering the Financing of Terrorism (AML/CFT) regime and in turn, implement the necessary policy responses to support the swift and effective implementation of measures to mitigate these emerging threats.

Impact of COVID-19 on AML/CFT Regimes

The introduction of social distancing and confinement measures designed to curb the spread of COVID-19 have negatively impacted financial institutions' ability to effectively meet their AML/CFT obligations. Significant numbers of governments and private sector employees have been reassigned, laid off or work remotely. Therefore, a significant shift in resources has been experienced in response to the COVID-19 crisis.

The COVID-19 pandemic's effect on the following areas is dependent upon the extent of the outbreak in the jurisdiction:

1.Supervision: AML/CFT onsite examinations have been postponed or substituted with desk-based inspections which decreases the level of onsite monitoring exhibited to financial institutions.

2.Regulation and Policy Reform: Governmental Agencies and private sector institutions have enacted and revised Continuity Plans to include COVID-19 countermeasures. Additionally, decision making bodies such as Board of Directors and legislative authorities have had to pause or reschedule the completion of necessary AML/CFT policies to prioritize COVID-19 issues.

3. *Law Enforcement Authorities:* A heightened focus has been placed on the enforcement of COVID-19 guidelines. Ongoing prosecutions, trials and hearings have been delayed or suspended.

Money Laundering Threats Associated with COVID-19

Measures taken by Governments and private sector entities across the world to relieve the threat of COVID-19 have inadvertently created new opportunities for criminals and terrorists to generate and launder illicit proceeds.

- Use of Online Platforms for Work and Social Interaction;
- Increased online sales;
- Increase in demand for medical supplies such as masks and ventilators;
- Reduced Face to Face Transactions in Banks and other financial institutions; and
- Mass Unemployment due to lockdown and lay offs.

Fraud Schemes

Criminals have attempted to benefit from the COVID-19 pandemic through fraudulent activities including the following:

* *Impersonation of Officials:* Criminals contact individuals via email or phone purporting to be government or hospital officials with the malicious objective of obtaining personal banking information or cash.
* *Counterfeiting:* These schemes include suspects selling illegal products, "miracle cures" and treatments. Similarly, persons are instructed to make payments and collect goods at bogus locations. Persons pretending to be employees of pharmaceutical vendors request payment for medical supplies such as masks, ventilators and testing kits. In some cases, the goods never arrive and in other cases, the goods arrive but are defective or counterfeit.
* *Fundraising for Fake Charities:* Emails from criminals from international organizations and charities are circulated requesting donations for COVID-19 related campaigns. The recipients are instructed to enter credit card information or to make direct payments through the suspects' digital wallets.

Cyber Crimes

There has been a marked increase in social engineering attacks using phishing email and mobile messages. These targeted attacks use links to fraudulent websites or attachments to obtain payment information.

Criminals forward emails and mobile messages to lure individuals into clicking malicious links and attachments granting them access.

Weaknesses in company network security are being exploited to obtain access to customer contact information and transaction records.

Cyber criminals use malicious websites and mobile applications to gain and lock access to devices (computers and phones) until payment information is seen and received.

Topics Discussed:

Other Money Laundering Vulnerabilities

1.Change in Financial Behaviours

Many financial institutions have closed offices, reduced operating hours and restricted some services especially those offered face to face. As a result, there has been a decrease in financial services including customer onboarding and identity verification. This can become concerning as some institutions may not be adequately equipped to identify customers' identity remotely.

Certain population segments such as the elderly, low income and indigenous communities may be less familiar with online platforms and are therefore more susceptible to fraud.

2. Misuse of Government Funding

Many Governments in the region have opted to providing stimulus packages (funds) to lessen the economic impact related to COVID-19. It has been reported that financial support offered to businesses and individuals may present potential fraud risks through the following ways:

* Criminals can claim to provide access to stimulus funds using fictitious websites, in order to obtain personal and financial information.

* Legal persons are used to create fraudulent claims by pretending to be legitimate businesses seeking financial assistance.

3. Increased Financial Volatility

Many economic and financial uncertainties arise from COVID-19. In this regard, criminals may shift their activities to exploit new vulnerabilities.

In the case of an economic downtown, criminals may seek to invest in troubled businesses to generate cash and mask illicit proceeds.

Recent fluctuations in the securities market have resulted in persons liquidating their portfolios and transferring large amounts of funds electronically.

The use of virtual assets can also assist criminals in laundering proceeds. The United States Justice Department has reported one (1) case where virtual assets were used to launder funds obtained from selling fraudulent COVID-19 medication.

Financing of Terrorism

The United Nations (UN) has cautioned that threats related to terrorism still remain and that terrorist groups may see and use opportunities for increased terrorist financing and terrorist activity while Governments' attention and priorities are focused on COVID-19.

Concerns have been raised that terrorist groups may seek to use the pandemic to raise and move funds and increase fraudulent activity to finance their operations.

Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) should therefore be cognizant of these opportunities and increase efforts to monitor the movement of client funds.

Regulatory Authority Responses

Jurisdictions across the region and the world have responded to the challenges posed by the COVID-19 crisis in an effort to maintain a high level of vigilance in addressing COVID-19 related financial crime risks.

- There should be strong domestic coordination to assess the impact of COVID-19 on AML/CFT risks and systems. Supervisors, the Financial Intelligence Unit (FIU) and Law Enforcement Agencies (LEAs) should work in tandem to provide guidance to the private sector. Additionally, AML/CFT Supervisors should engage with prudential supervisors to ensure appropriate prioritization of AML/CFT measures to address potential illicit activity related to COVID-19.

- There should be proactive engagement with the private sector to monitor the application of their AML/CFT procedures and policies and minimize potential impact.

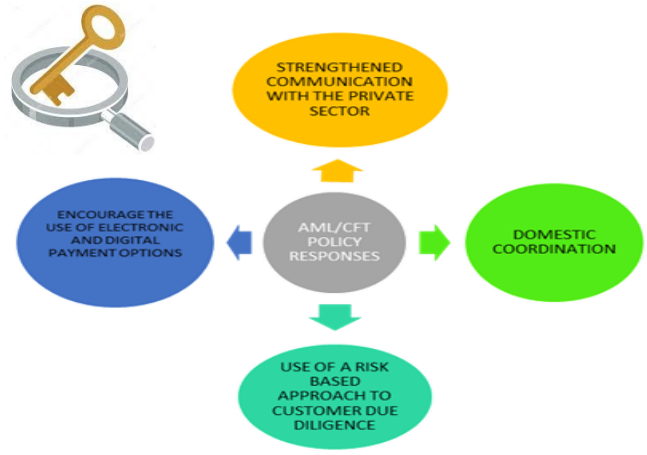
- Supervisors should encourage the use of appropriate digital identification tools with adequate assurance levels and other innovative solutions to assist in the identification of clients during the onboarding process and while transactions are being conducted.

- The use of electronic and digital channels should be encouraged to continue payment services while maintaining social distancing protocols.

- FIUs and Supervisors should continue to monitor the impact on reporting entities as the COVID-19 situation continues.

- Authorities must work together to understand and monitor the evolving risk environment. Agencies should consider pooling available resources to counteract the impact of COVID-19.

KEY FINDINGS



Criminals are taking advantage of the COVID-19 pandemic to carry out financial fraud exploitation scams that prey on virus related fears. Malicious or fraudulent cyber crimes, fundraising for fake charities and medical scams have increased. National authorities and international bodies are alerting citizens and businesses of these scams. Like criminals, terrorists may also exploit these opportunities to raise funds.

FIUs, AML/CFT Regulators and LEAs should continue to share information with the private sector to prioritize and address money laundering and terrorist financing risks.

References

World Health Organization https://www.who.int/emergencies/diseases/novel-coronavirus-2019

COVID-19 related Money Laundering and Terrorist Financing Risks and Policy Responses—Financial Action Task Force May 2020

South Independence Square Street, P.O.Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591 Fax: (869) 466-5317
Website: www.fsrc.kn / Email: info@fsrc.kn