



# Compliance Digest

Issue May 2020

# Compliance Digest

Issue May 2020



**Anil Fangoo, CAMS**  
Group Head Compliance  
and MLRO



Dear Readers,

Welcome to the May 2020 issue of our Compliance Digest which brings to you compliance and risk management related articles.

This issue gives you the necessary updates in the Acts, Regulations and Guidelines.

Readers will also benefit from articles such as EU List of Third Countries With Strategic Deficiencies in Their Anti-Money Laundering and Counter-Terrorist Financing Frameworks and Covid-19 related Financials Crime Risks: Fraud and AML Issues

We wish you a pleasant reading!

## In this issue



**Regulations**



**Compliance  
Highlight**



**Compliance  
Score**



**Global Score**



**Editorial Team:** Compliance & AML Team

# Recent Acts, Regulations, Rules & Guidelines

<b>Bank of Mauritius Guidelines</b>	<b>Effective Date/ Amendment Date</b>
Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation	January 2020
<b>Acts and Regulations</b>	
Financial Intelligence and Anti Money Laundering Regulations 2018 (as amended)	October 2018 (amended in May 2019)
United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019	May 2019
Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019	May 2019
The Covid-19 (Miscellaneous) Act 2020	May 2020
<b>Financial Services Commission</b>	
Anti-Money Laundering and Countering the Financing of Terrorism Handbook	January 2020

## **Main changes brought to the Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation**

- The Guideline has been revamped and it supersedes the previous Guidance Notes on AML/CFT (2017).
- It reflects the changes made in FIAMLA and FIAML Regulations in 2018.
- It provides more details on Terrorist financing, financial sanctions and proliferation financing.
- It reflects the requirements of the new United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019.
- It provides more details on Enterprise Wide Risk Assessment on AML/CFT.
- It clarifies on Risk Mitigation Measures to be implemented by banks.
- It provides more details on risk classification of clients, ongoing review and monitoring of clients.
- Relevant changes have been made to the KYC requirements of different type of customers.
- Simplified Due Diligence is no longer allowed by banks .
- Additional details on the Training Requirements of all relevant staff.

# Recent Acts, Regulations, Rules & Guidelines

## Main Key points on the Anti-Money Laundering and Countering the Financing of Terrorism Handbook ('Handbook') issued by the Financial Services Commission

- Details on Risk Based Approach is provided, whereby risk is broken down into Threat, Vulnerability and Consequence, understanding and application of principles relating to allocating weightage to the various risk factors such as Customer risk, Country risk, Product/Services/Transaction risk. For Customer Risk Assessment, tick box approach should be avoided and instead, FI must consider each customer on case-to-case basis, or in group risk-rated buckets, and look at risks they pose and their mitigating factors.
- Systems used to carry out electronic verification of natural persons is considered and guidance is provided on steps that could potentially be used to ensure the adequacy of the system.
- The Handbook also provides guidance on new and pre-existing products: digital information storage including cloud computing, electronic documentation storage, electronic verification of documentation, data and transaction screening systems and virtual/digital currencies.
- Guiding principle of all AML and CFT training for all directors, officers and employees to understand and accept their responsibility to contribute to the protection of the financial institution against the risks of money laundering/terrorism financing. Also, different employees need to have different levels of training based on responsibilities.

## Summary of the Financial Intelligence and Anti-Money Laundering Regulations 2018 (amended 2019)

The existing FIAMLA Regulations 2003 have been replaced with the Financial Intelligence and Anti-Money Laundering Regulations 2018 (the "Regulations") which came into force on 1 October 2018. This was subsequently amended in 2019, further to the proclamation of the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019. This improved the framework regarding Customer Due Diligence, Politically Exposed Persons, Correspondent Banking, Money or Value Transfer Services, New Technologies, Wire Transfers, Reliance on Third Parties, Internal Controls, Foreign Branches and Subsidiaries.

Additional details and clarifications were included in the Regulations concerning Enhanced Due Diligence to be conducted and the risk based approach to be used for High Risk Customers and PEPs.

Furthermore, as per the FIAML Regulations, where Financial Institutions are unable to perform CDD/EDD, they cannot

proceed with account opening and must therefore terminate the relationship and file a Suspicious Transaction Report. The regulations also included details on the internal controls and programmes against ML/TF risks to be implemented by FIs, including the following:

- designation of a compliance officer at senior management level for the implementation and ongoing compliance of the reporting person with internal programmes;
- screening procedures to ensure high standards when hiring employees;
- an ongoing training programme for its directors, officers and employees to maintain awareness of the laws and regulations relating to ML/TF; and
- an independent audit function to review and verify compliance with and effectiveness of the measures taken.

# Recent Acts, Regulations, Rules & Guidelines

## Summary of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

In 2019, Mauritius proclaimed the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (“UN Sanctions Act”). It enables the Government of Mauritius to implement targeted sanctions, including financial sanctions, arms embargo and travel ban, and other measures imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, with a view to addressing threats to international peace and security, including terrorism, the financing of terrorism and proliferation of weapons of mass destruction. As per the UN Sanctions Act, financial institutions in Mauritius have the following obligations:

- To regularly consult the Consolidated List and take

immediate action with respect to any changes brought thereto.

- regularly consult the newspapers for any notice which may be issued by the National Sanctions Secretariat and immediately act upon it.
- Financial prohibitions – Financial Institutions are not allowed to deal with the funds/assets of and make funds/assets available to parties listed by the United Nations.
- To implement internal controls and other procedures to enable it to effectively comply with the obligations of the Act and ensure proper reporting.

## Summary of the Anti-money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019

The AML&CFT Act was enacted with the view of meeting international standards of the FATF on anti-money laundering and combatting the financing of terrorism and activities related to the proliferation of weapons of mass destruction, by amending various enactments including the Companies Act 2001, the Banking Act 2004, the Financial Intelligence and Anti-Money Laundering Act 2002.



# Recent Acts, Regulations, Rules & Guidelines

## Summary of the Covid-19 (Miscellaneous Provisions) Act 2020



The COVID-19 (Miscellaneous Provisions) Bill and the Quarantine Bill were passed in the National Assembly on 16 May 2020 and received the assent of the President. The COVID-19 (Miscellaneous Provisions) Act aims at empowering the economy to weather this storm, save enterprises and jobs, and build for a recovery over time. The objectives of the Quarantine Act are to prevent the resurgence of COVID-19 infection, and step up the preparedness and response of the country to any future pandemic.

Main measures relevant to the banking sector are as per below:

### 1. COVID-19 Period

COVID 19 period defined as period from 23 March to 01 June 2020 or such further period as the Prime Minister may prescribe by way of regulations.

### 2. Macroeconomic Measures

Bank of Mauritius empowered to:

- grant such amount, as approved by its Board, to the Government to assist in the fiscal measures to stabilise the economy
- provide capital to or invest in any corporation or company set up for the purpose of facilitating economic development
- invest money in any corporation or company for the purpose of facilitating economic development, with the

approval of its Board, and

- to grant such amount from the Bank's Special Reserve Fund when requested by the Government and as approved by its Board, with the aim of assisting the Government to stabilise the economy

### 3. Companies and Reporting

Extension provided on annual meeting requirements and filing of financial statements obligations

### 4. Workers Right Act

Provision for Work from Home, Annual leaves, Protection from termination and Overtime during the Covid-19 period.



# Recent Acts, Regulations, Rules & Guidelines

## Summary of the Covid-19 (Miscellaneous Provisions) Act 2020 *(Continued)*

### 5. Insolvency Act:

- Changes in threshold of outstanding debt to file for bankruptcy by a debtor and for a creditor to petition for a debtor's bankruptcy.
- Resolutions to put a company in insolvent voluntary winding up or to put the company in liquidation, during COVID 19 period or three months thereafter, will be considered as no effect and void.
- Threshold of outstanding debt to serve a statutory demand increased.
- Time for compliance with statutory demand has been increased.

### 6. Mauritius Revenue Act:

- Extension until 25 June 2020 granted for any payment under a Revenue Law for a payment which falls due during the COVID 19 period.
- If time to make the payment falls during the period ending 30 June, the payment must be made not later than 26 June 2020.

### 7. Income Tax Act

Details provided on the contribution to COVID 19 Solidarity Fund, Wage Assistance Scheme and Covid-19 levy.

### 8. Registration Duty and Land (Duties and Taxes):

- Waiver of penalties and extension of time for submission of registrable documents or payment of registration where deadlines have fallen during the COVID 19 period or such other period as may be specified.
- Extension of the prescribed timelines relating to the procedure to object to the valuation of transfer of

shares where deadlines have fallen during the COVID 19 period or a specified time thereafter.

- Extension of the time limits applicable to various stages of the reassessment procedure of the valuation of transfer of immovable property, where they have fallen during the COVID 19 period or a specified time thereafter.

### 9. Landlord and Tenant Act

Non-payment of rent for the months of March, April, May, June, July and August 2020 will not amount to a breach of tenancy agreement, provided that such rent is paid in instalments by 31 December 2021.

### 10. Courts Act

Broader powers to the Chief Justice to administer any Court.

### 11. Data Protection Act

Relevant sections amended so as not to impede the collection, verification and processing of personal data for the issuance of licences permits and authorisations.

### 12. Passport and Immigration

Changes made in validity period of visas and permits which are expiring.

### 13. CEB and CWA Acts

No surcharge will be applicable in respect of water and electricity bills that fell due during the COVID 19 period or later period as may be prescribed and no there shall be no disconnection due to non-payment of such bills during the COVID 19 period.

## EU list of third countries with strategic deficiencies in their Anti-money Laundering and Counter-Terrorist Financing Frameworks

The European Commission's Anti-Money Laundering Package ('the Commission') of July 2019 highlighted a number of weaknesses in the EU's anti-money laundering / countering the financing of terrorism framework. To be able to address the issues highlighted, EU has worked an action plan to better enforce, supervise and coordinate the EU's rules on combating money laundering and terrorist financing. As one of their action points, the Commission has adopted a new list of third countries with strategic deficiencies in their anti-money laundering and counter-

terrorist financing frameworks and Mauritius is included in this list.

This inclusion follows the Eastern and Southern Africa Anti-Money Laundering Group's ("ESAAMLG") 2018 Mutual Evaluation Report on the Anti-Money Laundering Framework in force in Mauritius, further to which Mauritius was placed on a list of 'monitored jurisdictions' by the Financial Action Task Force ("FATF") in February 2020.

### ESAAMLG's 2018 Mutual Evaluation Report on the Anti-Money Laundering Framework

On 21 September 2018, the ESAAMLG published the Mutual Evaluation Report ("MER") following its assessment of Mauritius's level of compliance with the FATF Forty Recommendations and the level of effectiveness of its AML/CFT system. The report analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Mauritius' AML/CFT system, and provides recommendations on how the system could be strengthened.

Some of the major weaknesses identified are as per below:

- At the country level, there is no shared understanding of ML/TF risks facing the country.
- Financial institutions (FIs) demonstrated an understanding of ML/TF risks albeit at varying degrees, depending on size and level of sophistication of business operations.
- FIs operating in the global business sector are legally subject to AML/CFT obligations. However, the compliance responsibilities for FIs lie almost wholly on Management Companies (MCs), except in the case of banks, which results in a significant concentration of risks. Apart from potential conflict of interests, the number of clients against the resources of the MCs is also a matter of concern.
- The banks lead the way on filing of suspicious transaction reports (STRs), distantly followed by MCs. However, the level of STR reporting, particularly from

FIs in the global business sector and DNFBPs (Designated Non-Financial Businesses and Professions) is very low which is a concern given the size of the sectors and ML/TF risk exposure.

- Supervisory authorities have not adopted robust systems to assess ML/TF risks in individual FIs and across sectors which would inform an integrated and comprehensive risk-based supervision consistent with the dynamics of the global business sector.

Mauritius made various changes in the relevant laws, regulations and the regulatory and supervisory frameworks to address the issues identified as per the MER, in line with FATF requirements. Mauritius has, as at November 2019, submitted two follow up reports as well as two applications for technical compliance re-rating to the ESAAMLG, which were considered at its April 2019 and September 2019 meetings.

In April 2019, Mauritius was successful in obtaining technical compliance re-rating on 11 Recommendations and at the ESAAMLG Council of Ministers Meeting held in September 2019, Mauritius was successful in obtaining technical compliance re-rating on 19 Recommendations. In light of these two re-rating exercises, Mauritius has been rated Compliant or Largely Compliant on 35 of the 40 FATF Recommendations.



## EU list of third countries with strategic deficiencies in their Anti-money Laundering and Counter-Terrorist Financing Frameworks *(Continued)*

### FATF List - Jurisdictions under Increased Monitoring

In February 2020, Mauritius was included in the list of Jurisdictions under Increased Monitoring by FATF. When FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring.

The FATF recognises that Mauritius has taken measures to enhance the transparency of legal persons by amending the legal framework to require legal persons to disclose beneficial ownership information and improve the processes for identifying and confiscating proceeds of crimes.

Mauritius has also made significant efforts to increase the level of effectiveness of its Anti Money Laundering and Countering the Financing of Terrorism (AML/CFT) system by completing its National Risk Assessment in 2019, enhancing domestic coordination and international cooperation, developing and implementing an AML/CFT risk-based supervision framework for financial institutions and the implementation of the United Nations targeted financial sanctions related to terrorism and proliferation.

In February 2020, Mauritius made a high-level political commitment to work with FATF and ESAAMLG to strengthen the effectiveness of its AML/CFT regime and work on the following pending actions points:

1. demonstrating that the supervisors of its global business sector and DNFBPs implement risk-based supervision
2. ensuring the access to accurate basic and beneficial ownership information by competent authorities in a timely manner
3. demonstrating that Law Enforcement Agencies (LEAs) have capacity to conduct money laundering investigations, including parallel financial investigations and complex cases
4. implementing a risk based approach for supervision of its Non Profit Organisation (NPO) sector to prevent abuse for terrorist financing (TF) purposes, and
5. demonstrating the adequate implementation of targeted financial sanctions through outreach and supervision.

### Way forward

Concerning the Banking sector, it is worth highlighting that as per the MER, no strategic deficiency was identified. The report clarifies that most banks applied standards which

went over and above regulatory requirements. Moreover, as per NRA (2019) the Money Laundering Threat for the banking sector has been assessed as High due to its exposure risk and vulnerabilities. However, the assessment noted that the vulnerabilities are mitigated by strong AML controls in place in the banking sector, both at market entry and through preventive measures. Therefore, the residual ML vulnerability for the banking sector is medium.

This matter was part of the Parliamentary Debates held on 13 May 2020. The Minister of Financial Services and Good Governance highlighted that the following measures are being taken to expedite the implementation of the FATF Action Plan –

- A High Level Multi-Stakeholders Committee, chaired by the Prime Minister as well as the National AML/CFT Committee through regular reporting by its subcommittees are overseeing the implementation process.
- The Ministry of Financial Services and Good Governance is coordinating the implementation of the FATF Action Plan to ensure that Mauritius exits the FATF list at the earliest. The six sub-committees established under the National AML/CFT Committee are already submitting progress reports weekly.
- Technical assistance programmes under the EU funded Anti-Money Laundering and Combatting the Financing of Terrorism Global Facility and the German Government through the German Development Agency (GIZ) have been finalised and extensive engagements with relevant authorities are currently taking place to implement the FATF Action Plan.
- The Ministry of Financial Services and Good Governance has engaged with the EU for further technical assistance, as provided in the Regulation for listing High Risk Third Countries, to assist Mauritius to expeditiously complete the implementation of the FATF Action Plan.
- The Ministry of Financial Services is also working closely with the ESAAMLG.
- The Mauritian Authorities delivered on their commitment and a first progress report was sent to the FATF on the agreed date. Regrettably, the FATF process has been halted due to the Covid-19 situation and the progress report could not be assessed.
- A Risk Based Approach Framework for effective supervision by relevant authorities has been developed and is being implemented by the FSC.
- The Ministry has set up a team to work on the impact assessment of the EU listing.

# Compliance Score

## EU list of third countries with strategic deficiencies in their Anti-money Laundering and Counter-Terrorist Financing Frameworks *(Continued)*



### Way forward *(Continued)*

The Government remains committed to its objective of upholding the status of Mauritius as a financial hub abiding by the highest international principles. All relevant stakeholders, including the banking sector, will have to work together so as to ensure that we address these issues with the highest priority and to ensure compliance with the FATF Recommendations. Mauritius will have to demonstrate, as it has done several times in the past that, that it continues to operate by the highest standards of international good governance and regulatory framework.

The Mauritius Bankers Association issued a communique to clarify that no strategic deficiencies were identified in relation to the Banking sector, while the Ministry of Financial Services and Good Governance mentioned in its press release that the Government of Mauritius reiterates its high level political commitment to implement the action plan of the FATF at the earliest. Furthermore on 16 May 2020, the Financial Intelligence Unit has issued draft guidelines for consultation, to assist Attorneys, Barristers, Notaries, Jewelers and the Real Estate Sector in complying with their obligations under the FIAMLA.

## COVID-19-Related Financial Crime Risks: Frauds & AML issues

In these uncertain and difficult times, criminals and fraudsters are opportunistically preying on the confusion and panic created by the pandemic, and looking to profit from the public's desire to regain a sense of safety and security.

Authorities like The Financial Action Task Force, The Federal Bureau of Investigation, The Financial Crimes Enforcement Network, Financial Conduct Authority and Interpol issued guidance for consumers on COVID-19 related scams, noting that scams may take many forms. They may relate to insurance policies, pension transfers, or

high-return investment opportunities, including investments in crypto assets and furthermore scammers are sophisticated, opportunistic, persistent and very likely to target the vulnerable.

Many regulators across the globe have also realised the challenges that banks and other financial institutions will face in anti-money laundering compliance. They have instructed financial institutions to stay cautious and suggested certain best practices to counter an expected surge in money laundering operations.



### AML and CDD

This global health emergency has suspended business norms. With more regulated sector professionals working exclusively from home and client relationships entirely online, bank's customer due diligence (CDD) and anti-money laundering procedures (AML) will be affected. There may be new challenges for banks in running AML and CDD activities remotely or on site but with drastically downsized teams due to social distancing measures.

Banks have been advised to remind their relevant employees and agents/introducers that although the office is empty, customer risk assessment and CDD, extending to verification of individual and corporate clients, including beneficial owners must still be performed before any business relationship commences. Additional controls must be put in place in cases where the bank is unable to meet clients face to face. Moreover, a risk based approach must be used and high risk clients must be closely monitored.

Banks must also continue to conduct transaction monitoring and ongoing review of clients. Banks must look at red flags, for example why a customer/company is doing so much cash transactions during this timeframe when we currently have a lockdown and the client is a non-essential service provider. On the other hand, there are some businesses which will have a peak in the number and amount of transaction during this timeframe because they are an essential service provider, like a pharmacy or super markets and this is justified and must be properly documented.



### Frauds - Money Mules

Criminals and fraudsters are taking advantage of the uncertainty and fear surrounding the COVID-19 pandemic to steal people's money, access their personal and financial information, and use these people as a money mule.

Using people as a money mule starts off as a harmless and simple request. For example, an individual receives an email, through an online job site or a dating website. Then the individual is requested to provide his bank account information and allow money transfers to flow through the account. Once the individual received the money, he is then requested to move the money to someone else and the individual is paid a small amount of money for his help or he received another non-monetary benefit. This may look like ordinary financial activity. However, in reality these transfers are movement of illicit funds and these individuals whose accounts are being used they are not even aware that they are handling illicit funds. Acting as a money mule and allowing others to use your bank account, or conducting financial transactions on behalf of others does not only jeopardizes your financial security and compromises your personally identifiable information, but is also a financial crime.



### Other frauds

Other types of common frauds include advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that prey on virus-related fears. These frauds also include malicious or fraudulent cybercrimes, fundraising for fake charities, and various medical scams targeting innocent victims. These frauds are increasing globally, with criminals attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about COVID-19. Like criminals, terrorists may also exploit these opportunities to raise funds. Some examples as per table in the next page:



## COVID-19-Related Financial Crime Risks: Frauds & AML issues *(Continued)*

Frauds	Details
Medical supplies	With surgical masks, sanitisers, personal protection products and other medical supplies in high demand yet difficult to find in retail stores, fake shops, websites, social media accounts and email addresses claiming to sell these items have sprung up online. But instead of receiving the promised masks and supplies, unsuspecting victims have seen their money disappear into the hands of the criminals involved.
Phone frauds	Criminals are also using telephone deception to carry out financial frauds – they will call victims pretending to work for a hospital or medical clinic, claiming that a relative of the victim has fallen sick with the virus and request payments for medical treatment.
Phishing	Emails claiming to be from national or global health authorities, with the aim of tricking victims to provide personal credentials or payment details, or to open an attachment containing malware.
Business email compromise scams	After exploiting weakness in the business network security and gaining access to customer information, fraudsters would then request for payment to illicit bank account while impersonating counterpart of customer.
Identity thefts and malicious websites	These involves fraudsters emailing potential victims and pretending to be from organisations working with the WHO (World Health Organisation) and CDC (Centers for Disease Control and Prevention). The fraudsters claimed to be able to provide a list of infected people in the victim’s area. The victims were then asked to click on links to malicious websites in order to obtain the lists and were at times asked to make payments in Bitcoin.
Cyber threats	Cybercriminals are attacking the computer networks and systems of individuals, businesses and even global organizations at a time when cyber defences might be lowered due to the shift of focus to the health crisis. Main types of cyber-attacks being used are malicious domains, malware and ransomware and they are using Covid-19 terms and targeting hospitals, medical centres and public institutions.
Investment fraud	Victims are pressured into investing in fraudulent or worthless shares.
Loan sharks	Individuals and businesses on reduced incomes potential targets of loan sharks

### Other areas of financial crimes

The following areas of criminal exploitation where the banking system may be more vulnerable during the COVID-19.

- Targeting of government assistance programs through fraudulent applications and phishing scams.
- Economic Downturn – Criminals may invest illicit funds into troubled businesses in private sector business impacted by crisis in the long-term and not having access to trusted credit facilities.
- Movement of large amounts of cash following the purchase or sale of illegal or stockpiled goods.
- Out of character purchases of precious metals and gold bullion.
- Exploitation of workers or trafficking of vulnerable persons in the community.

- An increase in the risk of online child exploitation following restrictions on travel.
- Increased drug commerce via social media, encrypted apps and the Dark-net.

### Suspicious Transactions

Due to the pandemic and lock-down, bank may be facing major operational challenges that could impact their ability to conduct checks and report suspicious transactions. Banks must however continue to meet their anti-money laundering obligations, in particular the monitoring and reporting of suspicious transactions related to COVID-19.

## COVID-19-Related Financial Crime Risks: Frauds & AML issues *(Continued)*

### FATF Paper on COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses

#### A brief of the aforementioned FATF Paper is as follows:

As the world is focusing on responding to the COVID-19 pandemic, it is impacting on the ability of government and the private sector to implement anti-money laundering and counter terrorist financing (AML/CFT) obligations in areas including supervision, regulation and policy reform, suspicious transaction reporting and international cooperation. This could lead to emerging risks and vulnerabilities that could result in criminals finding ways to:

- Bypass customer due diligence measures;
- Increase misuse of online financial services and virtual assets to move and conceal illicit funds;
- Exploit economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;
- Increase use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;
- Misuse and misappropriation of domestic and international financial aid and emergency funding;
- Exploit COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.

AML/CFT policy responses can help support the swift and effective implementation of measures to respond to COVID-19, while managing new risks and vulnerabilities. This paper provides examples of such responses, which include:

- Domestic coordination to assess the impact of COVID-19 on AML/CFT risks and systems;
- Strengthened communication with the private sector;
- Encouraging the full use of a risk-based approach to customer due diligence;
- Supporting electronic and digital payment options.

#### Recommendations

According to the FATF, criminals and terrorists may seek to exploit gaps and weaknesses in national AML/CFT systems, under the assumption that resources are focused elsewhere. This makes risk-based supervision and enforcement activity more critical than ever.

Banks and other financial institutions must continue to work closely with their regulators, supervisors, financial intelligence units, law enforcement authorities and other relevant agencies in carrying-out their AML/CTF duties. Financial institutions and other businesses must also remain vigilant to emerging ML and TF risks and ensure that they continue to effectively mitigate these risks and are able to detect and report suspicious activity. FATF also encouraged the responsible use of digital identity, other responsible innovative solutions provided by FinTech companies in process of customer identification at on-boarding and in transaction monitoring.

Banks must also continue to sensitize their staff and clients to be careful and vigilant while conducting payments or processing transactions. Clients must be informed that they must not disclose their bank details on unsecured platforms and must not open emails or click on links which are unknown to them. It is also important to be cautious when doing online shopping and purchases. They may independently verify the company/individual offering the items before making any purchases. In cases clients or staff of the bank identify any type of fraud, they must escalate same immediately and such cases must be reported to relevant authorities.

www.fatf-gafi.org. (n.d.). *Jurisdictions under Increased Monitoring – 21 February 2020*. [online]

**Available at:** <http://www.fatf-gafi.org/countries/#other-monitored-jurisdictions>

THE UNITED NATIONS (FINANCIAL PROHIBITIONS, ARMS EMBARGO AND TRAVEL BAN) SANCTIONS ACT 2019 [online]

**Available at:** <http://mauritiusassembly.govmu.org/English/acts/Documents/2019/act0819.pdf>

Financial Intelligence and Anti-Money Laundering Regulations 2018 [online]

**Available at:** <http://www.fiumauritius.org/English/AML%20CFT%20Framework/Documents/2019/Financial%20Intelligence%20and%20Anti-Money%20Laundering%20Regulations%20No%20%20108%20of%202018%20updated%20June%202019.pdf>

COMMUNIQUE: European Commission lists Mauritius among high-risk jurisdictions. (n.d.). [online]

**Available at:** <http://www.mba.mu/pdf/2020/Mauritius-on-European-Commission-english%20version.pdf>

COMMUNIQUE European Commission List of High Risk Third Countries. (n.d.). [online]

**Available at:** <http://financialservices.govmu.org/English/Documents/2020/Press%20release%20-09.05.2020.pdf>

SEVENTH NATIONAL ASSEMBLY PARLIAMENTARY DEBATES (HANSARD). (n.d.). [online]

**Available at:** <http://mauritiusassembly.govmu.org/English/hansard/Documents/2020/hansard112020.pdf>

www.fiumauritius.org. (n.d.). *FIU - Home*. [online]

**Available at:** <http://www.fiumauritius.org/English/Pages/default.aspx>

Mutual Evaluation Report of Mauritius- Mutual Evaluation Report Mauritius Anti Money Laundering and counter-terrorist financing measures. (2018). [online]

**Available at:** <https://www.bom.mu/sites/default/files/AML/MER%20of%20Mauritius-July%202018.pdf>

www.fatf-gafi.org. (n.d.). *Statement by the FATF President: COVID-19 and measures to combat illicit financing*. [online]

**Available at:** <http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html>

www.fatf-gafi.org. (n.d.). *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*. [online]

**Available at:** <http://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html>

Federal Bureau of Investigation. (n.d.). *FBI Urges Vigilance During COVID-19 Pandemic*. [online]

**Available at:** <https://www.fbi.gov/coronavirus>

www.treasury.gov. (n.d.). *The Office of Foreign Assets Control (OFAC) Encourages Persons to Communicate OFAC Compliance Concerns Related to the Coronavirus Disease 2019 (COVID-19)*. [online]

**Available at:** <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200420.aspx>

www.fincen.gov. (n.d.). *The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic | FinCEN.gov*. [online]

**Available at:** <https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial>

Interpol.int. *COVID-19*. [online]

**Available at:** <https://www.interpol.int/en/How-we-work/COVID-19>

Bank of Mauritius website [online]

**Available at:** <https://www.bom.mu/>

Financial Services Commission Mauritius website [online]

**Available at:** <https://www.fscmauritius.org/en>





Compliance Digest is a newsletter issued by the Compliance Department of AfrAsia Bank Limited to provide updates and important compliance and risk management issues.

The editors welcome ideas for articles in future issues. Please send your ideas or submissions to Anil Fangoo at [Anil.Fangoo@afasiabank.com](mailto:Anil.Fangoo@afasiabank.com)

---



Follow Us on

