MANDATORY ML/TF/PF RISK ASSESSMENT ON NEW TECHNOLOGIES

AML/CFT/P Guidance Note 1 of 2024

for Non-Bank Financial Institutions

February 26, 2024

Disclaimer

This Guidance Note is issued by NBFIRA in line with section 49 (1) c of the Financial Intelligence Act and Regulations 2022 ("FI Legislation") of the Republic of Botswana for comprehensive use by the NBFIs. The note is indicative and while due care was exercised to ensure that its contents are accurate and consistent with the FI Legislation, the latter shall prevail in the unfortunate case of ambiguity and the NBFIRA does not guarantee or take any liability whatsoever.

Table of Contents

1. Introduction

1.1. In accordance with section 13(1)(c) of the Financial Intelligence Act of 2022, it is mandatory for non-bank financial institutions (NBFIs) to conduct a Money Laundering/Terrorist Financing/Proliferation Financing (ML/TF/PF) risk assessment of any new technologies they intend to introduce. The rapid advancement of technology has brought about innovative solutions in the financial sector, presenting both opportunities and challenges.

1.2. It is, therefore, imperative for NBFIs to thoroughly assess the ML/TF/PF risks associated with new technologies before their implementation to mitigate potential risks and ensure regulatory compliance.

1.3. Accordingly, the guidance note is issued in accordance with section 5 (2) (d) of the Non-Bank Financial Institutions Regulatory Authority Act of 2023 (NBFIRA Act) read with section 49 (1) (c) of the FI Act as a reminder and guideline for compliance with the requirement. It should also be read in conjunction with other guidance notes issued by the Authority, more especially guidance note No. 4 on Conducting an Institutional Risk Assessments.

2. Background

2.1. NBFIs regularly introduce various new technologies into their businesses to enhance efficiency, improve customer satisfaction, and stay competitive in the market. Some of these technologies may introduce vulnerabilities that could be exploited for money laundering (ML), terrorism financing (TF) and proliferation financing (PF) purposes.

2.2. The guidance note is a concise NBFIs and outline to the clear instructions regarding the requirement to assess the ML/TF/PF risks associated with new technologies before adoption to mitigate potential risks and ensure regulatory compliance. It serves as a

practical resource for financial institutions to understand and fulfill their obligations regarding ML/TF/PF risk assessment on new technologies.

3. New Technologies

3.1. Some examples of new technologies that NBFIs regularly introduce are outlined and explained below.

3.1.1. *Mobile Payments and Digital Wallets*

Mobile payment platforms and digital wallets facilitate quick and convenient transactions, but they may also be susceptible to misuse for ML/TF purposes, especially if proper customer identification and verification measures are not effective.[1]

3.1.2. *Peer-to-Peer (P2P) Lending Platforms*

P2P lending platforms enable individuals and businesses to lend and borrow money directly, bypassing traditional financial institutions. These platforms may be exploited for ML/TF/PF by facilitating anonymous transactions and concealing the true source of funds.

3.1.3. *Artificial Intelligence (AI) and Machine Learning*

AI and machine learning technologies are increasingly used by financial institutions for fraud detection, customer profiling, and risk management. However, these technologies may also be exploited by criminals to evade detection and conduct ML/TF/PF activities.

3.6 **The dark web** refers to a part of the internet that is not indexed by traditional search engines and requires specific software, configurations, or authorization to access. It is often associated with illicit activities due to its anonymity and lack of oversight. The dark wed is used for various purposes, including illegal trade in drugs, weapons, stolen data, and other contraband, as well as for communication and collaboration among cybercriminals. **Tor**, short for "The Onion Router" is a network that enables anonymous communication over the internet. It uses a distributed network of servers called nodes to route internet traffic through multiple nodes makes it difficult to trace the origin and destination of internet traffic, providing users with a high degree of anonymity.

3.1.4. *Remote Account Opening and Digital Onboarding*

Remote account opening and digital onboarding processes streamline customer acquisition but may also introduce vulnerabilities if proper identity verification and due diligence procedures are not followed, allowing criminals to open accounts under false identities.

3.1.5. *Virtual Asset Service Providers (VASPs)*

VASPs, including virtual currency exchanges and wallet providers, are susceptible to ML/TF/PF risks due to their involvement in facilitating the exchange, storage, and transfer of virtual assets, including cryptocurrencies.

3.1.6. *Dark Web and Tor Networks*

Financial institutions may inadvertently introduce vulnerabilities by accessing or utilising dark web marketplaces or Tor networks for legitimate purposes, as these platforms are known for facilitating illicit transactions, including ML/TF activities.

4. Guidelines for ML/TF Risk Assessment of New Technologies

4.1. It is essential for financial institutions to conduct thorough ML/TF/PF risk assessments of these and other new technologies before their adoption to identify and mitigate potential vulnerabilities effectively. Additionally, ongoing monitoring and review of these technologies are crucial to adapt to evolving ML/TF threats and regulatory requirements.

4.2. *Identification of New Technologies*

Financial institutions must identify and document all new technologies proposed for implementation within their operations. In doing so they must consider the following factors:

(a) Nature and complexity of the technology
(b) Integration with existing systems and processes
(c) Customer identification and verification methods
(d) Transaction monitoring capabilities

(e) Data privacy and security measures

(f) Jurisdictional risks associated with the technology's deployment.

4.3. *Assessment of ML/TF/PF Risks*

Conduct a comprehensive ML/TF risk assessment specific to each new technology. This assessment should evaluate potential vulnerabilities, threats, and risks associated with ML/TF activities.

4.4. *Engagement of Relevant Stakeholders*

Ensure active involvement of relevant stakeholders such as IT departments, compliance officers, risk managers, and legal counsel during the risk assessment process.

4.5. *Documentation and Reporting*

Document all findings and conclusions of the ML/TF risk assessment in a comprehensive report of new technology. Submit the report to the Regulator for review and approval upon request.

4.6. *Mitigation Measures*

Develop and implement appropriate mitigation measures to address identified ML/TF risks effectively. These measures may include enhanced due diligence procedures, transaction monitoring protocols and ongoing risk assessments.

4.7. *Ongoing Monitoring and Review*

Establish mechanisms for ongoing monitoring and review of the effectiveness of the implemented risk mitigation measures. Regularly update the ML/TF risk assessment in response to changes in technology, regulations, and emerging threats.

5. Conclusion

5.1. By issuing this Guidance Note, the Authority anticipates improved compliance, proactive risk management, and awareness of regulatory requirements within the financial industry with regards to new technologies.

6. Authorisation

6.1. This Guidance Note was reviewed and approved on February 26, 2024 and applies immediately.