NIGERIAN FINANCIAL INTELLIGENCE UNIT

GUIDANCE NOTE

NFIU/EXT/PUB/GUIDE/AC-STEI/MAR-2022/VOL.I/001

EXECUTIVE SUMMARY ON ROYAL UNITED SERVICES INSTITUTE (RUSI) GUIDANCE ON COUNTERPROLIFERATION FINANCING FOR VIRTUAL ASSET SERVICE PROVIDERS (VASPs)

The Nigerian Financial Intelligence Unit (NFIU) In fulfilment of its obligations on the timely provision of guidance to Reporting Entities and Competent Authorities (CA) publishes Indicators and advisory on crimes of money laundering and terrorist financing in an effort to guide Reporting Entities and Competent Authorities on observable trends and patterns to mitigate AML/CFT/CPF threats.

MARCH 2022

Contents

1. Introduction

Proliferation Financing (PF) of Weapon of Mass Destruction (WMD) is defined by the Financial Action Task Force (FATF) as the act of providing funds or financial services which are used, in whole or in part, for the manufacturing, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons. It has become a major driver of growing insecurity concerns across the world while fueling insurgency, terrorism, human trafficking, organized crime, internal insurrections and civil wars among other destabilizing trends thus posing an obstacle to the sustenance of global peace and security. WMD proliferators in some countries continue to evade targeted financial sanctions and the use of virtual assets and virtual assets service providers (VASPs) have increasingly become a means through which proliferation-related funds are raised and moved.

This Executive Summary based on a guidance paper published by RUSI[1] (Izenman, 2021) will serve as a blueprint to VASPs) on financial crime compliance practice when dealing with PF risk and direct compliance officers towards relevant guidelines that will assist them in performing their duties. This guide will also assist VASPs who have not thought of PF or targeted financial sanctions implementation, towards proliferation as distinct financial crime and sanctions risks. This Executive Summary follows financial compliance cycle practices, beginning with pre-requirements before client interaction, and then moving to the on-boarding process, followed by ongoing monitoring throughout the client relationship. After going through the cycle, the guide touches on high-risk indicators and red flags that could lead to enhanced due diligence or exiting of the client and concludes with reporting requirements following any flagged suspicious activity.

2. FATF Recommendations for VA) and VASPs

Understanding the risk involved in VAs and VASPs is very key as regards Recommendation 15. The FATF interpretive notes on Recommendation 15 further clarifies how the FATF Recommendation applies to VAs and VASPs which includes, guidance on supervision, monitoring, licensing and registration, customer due diligence (CDD), suspicious transaction reporting and sanction screening measures. The FATF also adopted guidelines for a risk-

[1]**Royal United Services Institute** (RUSI) for Defence and Security Studies founded in 1831 is a long-standing UK based think tank devoted to inform, influence and enhance public debate on a safer and more stable world. Accessible on https://static.rusi.org/299_SR_CPF_VirtualAssetsGuide.pdf

based approach for VAs and VASPs in June 2019[2], which aims to assist national authorities in developing appropriate regulation regimes for VAs and VASPs, and also to advise the private sector on how to comply with these requirements.

3. Terminology

This Executive Summary uses vocabulary employed by the FATF. The term VAs and VASPs are used throughout. The scope of this summary is narrow to VAs and VASPs, while the FATF definition includes any business involved in VA-to-fiat exchange, VA-to-VA exchange, or the transfer, safekeeping, or administration of VAs, and any business providing financial services relating to VAs, this executive summary defines a VASP as a centralized virtual asset exchange offering VA-to-fiat or VA-to-VA services.

4. Methodology

The Executive summary is part of theRUSI's ongoing analysis on CPF. The Unit may want to domesticate this document as a guide for the role of VAs and other new payment systems play in sanctions evasion, money laundering, terrorism financing and other illegal activities in the country.

5. Pre-Requirements

Pre-Requirements in combating PF are financial crime compliance practices put in place before onboarding any customer. This includes an effective and knowledgeable compliance team, initial risk assessments, a thorough understanding of all relevant national and international requirements, proper cyber security training, protocols and policies.

6. Compliance Team

The VASP should have a proper governance structure and compliance team. Also, staff should be trained regularly on ML/TF/PF trends and typologies.

7. Risk Assessment

The VASP should conduct at least one comprehensive, documented risk assessment annually or as frequently as the transactions are done and have auctioned key control requirements to address high risks based on risk assessment outcomes.

[2] Guidelines for a risk-based approach for VAs and VASPs in June 2019

8. Cyber-Security

The VASP should put in place effective cyber-security protocols. In addition, an appropriate and comprehensive IT and Cybersecurity infrastructure should be in place. Staff should undergo regular cyber-security training.

9. Asset Listing Requirements

The VASP should have appropriate asset listing requirements e.g., like criminal players having an increasing interest in privacy coins, which potentially allow them to move VAs undetected, it is key to consider the blockchain tracing abilities for any asset being listed on a VASP's platform. There are a variety of options that may help mitigate risks posed by privacy coins. One option is simply to exclusively offer assets with transparent blockchains, in other words, not accepting any privacy coins at all.

10. Sanctions

Sanctions should be applied where necessary to all customers and transactions, no matter the amount involved. VASPs should fully adhere to international and relevant national sanctions lists to avoid holding accounts for designated players or anyone owned, controlled, acting on behalf of or at the direction of designated players. Sanctions screening should be conducted at the stage of first identity verification and maintained throughout the customer relationship. When there are additions to transaction lists, VASPs should also screen for players included in UN Panel of Experts Reports. VASPs should also consult typology reports by NGOs as well as adverse media screening.

11. On-boarding

This is the second step in the compliance cycle. VASPs should introduce comprehensive and adequate Know Your Customers (KYC) processes i.e customer identification processes which require; the customer's full name, date of birth, nationality, and address. Customer personal information and addresses should be verified using official government identification documents, proof of address documents, or appropriate digital means. KYC and continual CDD (Customer Due Diligence) processes are conducted on any beneficial owners or persons acting on behalf of the customer. VASPs should also understand the extent of both the source and destination of any funds moved.

12. On-going Monitoring and Custom Due Diligence

This next stage is to ensure continued and effective CDD on existing customers. This means transaction monitoring to identify any unusual activity, such as deviation from expected or

anticipated transaction activity, and understanding the reasoning and purpose behind any variation that is found on the platform. All documents and information submitted to the VASP during onboarding are kept up to date throughout the relationship. VASPs should have an automated system put in place to comprehensively monitor sanctions screening and they should also carry out Enhanced Due Diligence (EDD) when a transaction or account is flagged as high risk or in a high-risk jurisdiction.

13. High-Risk Indicators and Red Flags

High-risk indicators and red flags may lead to EDD, STRs/SARs or even fund freezing. The FATF, the private sector and national regulators have all comprehensively listed identified red flags. VASPs should manage relationships with mixers and create an approved list of known or trusted mixers and CoinJoin[3] services under specific conditions.

14. Reporting Requirements

Reporting and filing of SARs/STRs are mandatory for the VASPs. They should be prepared to operate at the highest global standards alongside other regulated financial service providers and report all activities they find suspicious to the relevant authorities. They should be aware of and understand the FATF recommendations, understand and comply with the jurisdiction reporting requirements. A designated staff (compliance officer) should be assigned to ensure that the VASP adheres to and fulfills its reporting obligations and a standard internal reporting system should also be put in place for ease of understanding.

15. Recommendations

- **National Risk Assessment**: National risk assessments could be conducted to strengthen the CPF regime of the country.
- **Institutional risk assessment**: VASPs should be required to take appropriate steps to identify and assess their proliferation financing risks for customers, geographic areas, products, services, transactions and delivery channels.
- **Domestic co-operation, coordination and information sharing**: An inter-agency framework should be put in place to effectively mitigate proliferation financing risks. Effective co-operation and coordination among all the relevant departments, agencies and organizations, which are generally involved in combating proliferation

[3]CoinJoin is an anonymization strategy that protects the privacy of Bitcoin users when they conduct transactions with each other, obscuring the sources and destinations of BTC used in transactions (Hayes, 2021). Accessible on https://www.investopedia.com/terms/c/coinjoin.asp

and proliferation financing at the national level. E.g. import and export controls and licensing authorities, customs and border controls, intelligence agencies, financial sector regulators and other relevant regulators such as the Nigeria Nuclear Regulatory Agency (NNRA). Additionally, this guidance brief should be shared with all relevant stakeholders in Nigeria's AML/CFT/CPF regime to increase the level of awareness and understanding of CPF measures and the role of VASPs in countering the specific threat of PF.

- **Effective and adequate legal framework, licensing and registration**: Effective and adequate legal frameworks should be put in place to implement proliferation-related targeted financial sanctions without delay in line with Recommendation 7. Efforts should be made towards the licensing and registration of VASPs operating in Nigeria and a designated supervisor/regulator should be legislated to license and supervise their operations.
- **Reporting Obligations**: Once licensed to operate, VASPs ensure reporting of currency transaction reports (CTRs) and suspicious transactions/activities (STRs/SARs) to the NFIU in accordance with **section 3(1)(b) of the NFIU Act, 2018**.
- **Compliance monitoring and enforcement**: VASPs should be subject to supervision and monitoring to ensure full compliance with their targeted financial sanctions obligations by the NFIU and/or their supervisors/regulators.
- **Regular and in-depth training:** Regular and in-depth training of VASPs, financial institutions, regulatory authorities and other agencies involved in counter-proliferation financing, on proliferation financing, as well as Identifying priority areas for expanded training may advance the effective implementation of controls to mitigate the risks.