NFIU ADVISORY ON POTENTIAL ML/TF RISKS OF VIRTUAL CURRENCY

Contents

1. INTRODUCTION

In June 2014 the Financial Action Task Force (FATF) issued a report on Virtual Currencies Key Definitions and Potential AML/CFT Risks (June 2014 Virtual Currency Report).The FATF observed that virtual currency payment, products and services (VCPPS) present opportunity for money laundering and other crime risks that must be identified and mitigated.

In recent years, virtual currencies (VCôs) have emerged and attracted substantial investments in payment infrastructures built on their software protocols. These payment mechanisms seek to provide a new method for transmitting value over the internet. The FATF recognizes innovation; at the same time, believes VC payment products and services (VCPPS) present money laundering and terrorist financing (ML/TF) risk and other crimes that must be identified and mitigated. The commonwealth, World Bank and IMF recently formed the commonwealth Virtual currencies Working Group, charged with raising awareness, developing capacity among member states and providing technical guidance. The working group urges member government to review their legislative response to virtual currencies, such as Bitcoin, to ensure they address associated risks and avoid stifling innovation. Member states are also advised to consider the applicability of their existing legal frameworks to virtual currencies and where appropriate, they should enact new legislations to regulate the VC payment instrument.

Although the use of virtual currencies, especially convertible digital currencies like bitcoin, for transaction payments and speculative investments has seen rapid acceptance globally, it is still not issued or guaranteed in any jurisdiction, and in recent times, reports have shown that virtual currencies are highly vulnerable, allowing cyber criminals and corrupt official to abuse it.

2. DEFINITIONS

Virtual Currency is a digital representation of value that can be digitally traded and function as:

(1) a medium of exchange; and /or
(2) a unit of account; and/or
(3) a store of value, but does not have legal tender status (i.e,when tendered to a creditor, is not a valid and legal offer of payment) in any jurisdiction.

Virtual Currency is not issued nor guaranteed by any jurisdiction, though fulfils the above functions only by agreement within the community of users of virtual currency. Virtual currency is distinguished from flat currency (a.k.a. ñreal currency,ò ñreal money,ò or ñnational currencyò) which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country .it is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency i.e. it electronically transfers values that has legal tender status. **Digital currency** can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term ñvirtual currencyò

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back and forth for real currency. Examples include: Bitcoin, e-Gold (defunct), Liberty Reserved (defunct), Second Life Linden Dollars and web money.

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars, QCoins and World of War craft Gold.

3. PURPOSE

This advisory is intended to explain the application of the risk-based approach to AML/CFT measures in the virtual currency context; identify the entities involved in VCPPS in Nigeria; and clarify the application of the relevant FATF recommendations to convertible virtual currency exchangers. This guidance is also intended to educate national authorities to understand and potentially develop regulatory responses including the need to amend their law in other to address the potential ML/TF risks of VCPPS. This advisory is further intended to help the private sector better understand the relevant AML/CFT obligations on Virtual Currency and how they can effectively comply with relevant requirements. Importantly, the advisory incorporates the conceptual framework and key terms adopted by the FATF in its June 2014 VC Report. Readers are referred to that document for discussion of potential cases for VC and a glossary of terms.

This Guidance focuses on applying the risk based approach to ML/TF risks associated with VCPPS, and not on other types of VC financial products, such as VC securities or futures products. Accordingly, the guidance has adopted the term VC payments products and services (VCPPS), rather than VC products and services (VCPS), where the discussion is limited to VC payments schemes .The development of VCPPS and interactions of VCPPS with other New Payment Products and Services (NPPS) and even with the traditional banking services, give rise to the need for this guidance to protect the integrity of the domestic and global financial system. This Guidance builds on the June 2014 VC reports and on the risk matrix and the best practices of the Guidance for a Risks-Based Approach to Prepaid cards, Mobile Payment and Internet Based Payment Services report (June 2013 NPPS report).

The focus of this Guidance is on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers as we learn more about the technology and use of VCPPS, the Guidance may be updated, to include, where appropriate, emerging best practices to address regulatory issues arising in respect of ML/TF risks associated with VCPPS. It is in view of this observed development in the Nigeria financial sector that the NFIU is bringing this advisory to your attention, to serve as a guide for regulators, law enforcement officers, Digital currency operators in Nigeria,

financial institutions and designated non financial institutions in addressing issues related to Virtual Currency.

4. INITIAL RISK ASSESSMENT

The risk assessment in the FATF June 2014 VC report indicates that at least in the near-term, only convertible VC, which can be used to move value into and out of fiat currencies and the regulated financial system, is likely to present ML/TF risks. Accordingly, under **RBA,** countries are to focus their AML/CFT efforts on higher-risk convertible VCs. The risk assessment also suggests that AML/CFT control should target convertible VC nodes i.e. points of intersection that provide gateways to the regulated financial system and not seek to regulate users who obtain VC to purchase goods or services. These nodes include third-party convertible VC exchangers, where that is the case, they should be regulated under the FATF recommendations. Thus, countries are to apply relevant AML/CFT requirements specified by the international standards to convertible VC exchangers, and any other types of institution that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system. Under the RBA, countries should also consider regulating financial institution or DNFBP that send, receive and store VC, but do not provide exchange or cash-in/cash-out services between virtual and fiat currency. This is however not within the scope of this Guidance.

5. APPLICATION OF FATF STANDARDS TO COVERED ENTITIES

This section explains how specific FATF Recommendations should apply to Convertible VC exchanges and any other type of entities that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system, to mitigate the ML/TF risks associated with VCPPSs.

- **Recommendation 1**. The FATF Recommendations make clear that countries should require financial institutions and DNFBP to identify, assess, and take effective action to mitigate their ML/TF risks (including those associated with VCPPS). This includes on-going efforts to refine technical processes used to reliably identify and verify customers.

For AML/CFT purposes, where VC activities are permitted under national law, all jurisdictions, financial institutions and DNFPBs, including convertible virtual currency exchangers, should assess the ML/TF risks posed by VC activities and apply a RBA to ensure that appropriate measures to prevent or mitigate those risks are implemented. The RBA does not imply the automatic or wholesale denial of services to VCPPS without an adequate risks assessment.

- **Recommendation 10.** CDD is an essential measure to mitigate the ML/TF risks associated with convertible VC. In accordance with the FATF Standards, countries should require convertible VC exchangers to undertake customer due diligence when establishing business relations or when carrying out (non-wire) occasional transactions using reliable, independent source documents, data or information, For example, convertible VC exchangers should be required to conduct customer due diligence when exchanging VC for fiat currency or vice versa in a one-off transaction greater than the designated threshold of USD/EUR 15 000 of USD/EUR 15 000 or (b) carrying out occasional transactions that are wire transfers covered by **Recommendation 16** and its Interpretive Note. Usually, convertible VC transactions will involve a wire transfer and therefore be subject to **Recommendation 16**.

- Countries may wish to consider having a lower or no threshold for VC CDD requirements if appropriate, given the nature and level of identified ML/TF risks.

- In light of the nature of VCPPS, in which customer relationships are established, funds loaded and transactions transmitted entirely through the Internet, institutions must necessarily rely on non face-to-face identification and verification. Countries should consider requiring entities providing VCPPS to follow the best practices suggested in the June 2013 NPPS Guidance. These, to the extent applicable, include: corroborating identity information received from the customer, such as a national identity number, with information in third party databases or other reliable sources; potentially tracing the customerôs Internet Protocol (IP) address; and searching the Web for corroborating activity information consistent with the customerôs transaction profile, provided that the data collection is in line with national privacy legislation.

- Where convertible VCPPS are presenting higher risk, as ascertained on the basis of the RBA, convertible virtual currency exchangers should be required to conduct enhanced CDD in proportion to that risk, and encouraged to use multiple techniques to take reasonable measures to verify customer identity. Where convertible virtual currency exchangers are permitted to complete verification after establishing the business relationship in order not to interrupt the normal conduct of business (in low risk cases), they should be required to complete verification before conducting occasional transactions above the threshold.
- Countries should also expect financial institutions and DNFBP to consider risks associated with the source of funding convertible VCPPS. Decentralised convertible VCPPS allow anonymous sources of funding, including peer-to-peer (P2P) VC transfers and funding by NPPS that are themselves anonymous, increasing ML/TF risks. As with NPPS, VCPPS business should consider, for occasional transactions above a given threshold, limiting the source of funds to a bank account, credit or debit card, or at least apply such limitations to initial loading, or for a set period until a transaction pattern can be established, or for loading above a given threshold.

- Transaction monitoring is a key risk mitigating factor in the convertible VC space because of the difficulty of non-face-to-face identity verification and because it is only recently that decentralised convertible VC technology allows certain risk mitigating process that may be available for NPPS to be built into decentralised VCPPS in order to restrict functionality and reduce risk. For instance, multi signature (multi-sig) technology now enables VCPPS to effectively build in loading total wallet value, and value/velocity transaction limits into decentralised VCPPS. However, current decentralised VC technology does not make it possible to effectively build in geographic limits; limit use to the purchase of certain goods and services; or prevent person-to-person transfers.

- It is recommended that countries encourage transaction monitoring, commensurate with the risk. The public nature of transaction information available on the block chain theoretically facilitates transaction monitoring, but as noted in the June 2014 VC Report

(Appendix A), the lack of real world identity associated with many decentralised VC transactions limits the block chainôs usefulness for monitoring transactions and identifying suspicious activity, presenting serious challenges to effective AML/CFT compliance and supervision.

- **Recommendation 11, Recommendation 20 and Recommendation 22**. Recordkeeping and Suspicious activity reporting when VC transactions could involve the proceeds of criminal activity or be related to terrorist financing, in accordance with Recommendation 20, are also essential. At a minimum, financial institutions and DNFBP should be required to maintain transaction records that include: information to identify the parties; the public keys, addresses or accounts involved; the nature and date of the transaction, and the amount transferred. The public information available on the block chain provides a beginning foundation for record keeping, provided institutions can adequately identify their customers. Countries should require institutions to be attentive to the type of suspicious activity they are in a position to detect.

- **Recommendation 15 and Recommendation 22** specifically addresses new technologies and requires financial institutions and DNFBP to identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. **Recommendation 15** also requires financial institutions and DNFBP licensed by or operating in a jurisdiction to take appropriate measures to manage and mitigate risk before launching new products or business practices or using new or developing technologies. These measures apply in relation to VC as a new technology. National authorities are expected to enforce this obligation, and financial institutions and DNFBP should be proactive in fulfilling the expectations set forth in **Recommendation 15.**

6. POTENTIAL SOLUTIONS TO COMPLIANCE CHALLENGES

- Financial institutions and DNFBP should be required to comply with customer identification, verification and transaction monitoring requirements for decentralized convertible VCPPS, using the most effective and efficient means available, as soon as such products/services are offered. Given the compliance and law enforcement challenges presented by decentralized convertible VC, financial institutions, DNFBP, developers, investors, and other actors in the VC space should seek to develop technology-based solutions that will improve compliance.

- For example, developers may be able to create new VC technologies, such as application programming interfaces (APIs) that provide customer identification information, or allow financial institutions or DNFBP to limit transaction size and velocity or establish a variety of conditions that must be satisfied before a VC transaction can be sent to the recipient/beneficiary to reduce the ML/TF risks associated with a particular VCPPS. The possibility of using information collected online to augment the customer profile and help in detecting suspicious activity and transaction is another important AML/CFT compliance growth area. Innovation relevant to AML/CFT compliance may take the form of improving existing VC protocols or developing entirely new VCs, built on fundamentally different underlying protocols that can build-in risk mitigants or facilitate customer identification and transaction monitoring.

- Third-party digital identity systems may also be developed to facilitate AML/CFT compliance that might better fit VCPPS. These systems could, for instance, involve third-party digital identity custodians and/or other entitiesô creating, authenticating, and maintaining digital identity solutions for specific CDD, monitoring, and reporting purposes, in response to requirements imposed by national AML/CFT laws implementing the international standards. Third party digital identity custodians would themselves need to be regulated to ensure identification/verification integrity.

- Financial institutions and DNFBP could also explore developing business models to facilitate customer identification/verification, transaction monitoring, and compliance with other relevant AML/CFT requirements. For example, institutions involved in transmitting decentralised convertible VC could consider creating an industry association(s) composed of vetted VC institutions and develop policies and practices for members that allow them to identify specific transactions as coming from a member that has applied appropriate CDD and is conducting appropriate transaction monitoring.

REFERRENCES:

http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
http://www.virtualcurrencytoday.com/news/central-bank-of-nigeria-asks-for-virtual-currency-regulation/
http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

ACRONYMS

AML Anti-money laundering
ATM Automated teller machine
CDD Customer due diligence
CFT Countering the financing of terrorism
DNFBP Designated non-financial business and profession
FINMA Financial Market Supervisory Authority
MAS Monetary Authority of Singapore
ML Money laundering
MSB Money service business
MVTS Money value transfer service
NPPS New Payment Products and Services
P2P Peer-to-peer
RBA Risk-based approach
TF Terrorist financing
VC Virtual currency
VCPPS VC payment products and services