ST. KITTS BRANCH
Financial Services Regulatory Commission

NewsLetter

May 2021
Issue No. 84

VIRTUAL ASSETS: Vehicles for Financial Crime

Important Definitions

Virtual Assets (VAs) refer to digital representations of value that can be digitally traded, or transferred, and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account and/or a store of value. They do not include digital representations of fiat currencies, securities and other financial assets.

Virtual Asset Service Providers (VASPs) means any natural or legal person which as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. exchange between virtual assets and fiat currencies;
ii. exchange between one or more forms of virtual assets;
iii. transfer of virtual assets;
iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Blockchain is a type of distributive ledger, in which transactions are duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions. Each time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.

Brief History on FATF Guidance for Virtual Assets

In 2018, the Financial Action Task Force (FATF) published changes to its recommendations and glossary relating to VAs and VASPs. These changes supplemented the 2015 FATF report, Guidance for a Risk-Based Approach to Virtual Currencies which was built on the FATF's report Virtual Currencies Key Definitions and Potential AML/CFT Risks, in June 2014 (June 2014 VC report).

In June 2019, the FATF issued new guidance in the form of an interpretative note to its 40 Recommendations to further clarify the requirements which should be applied to VAs and VASPs. This guidance was issued to help national authorities in understanding and developing regulatory and supervisory responses to virtual asset activities and VASPs and the private sector in understanding their obligations in the prevention of financial crime when engaging in virtual assets activities. The guidance also helps private sector organizations to apply FATF requirements to businesses within the Financial Services sector.

In March 2021, in an effort to provide clear and more substantive guidance, the FATF published draft guidance on a risk-based approach to VAs and VASPs for public consultation. This revised document provides updated guidance in six (6) main areas to

(1) clarify the definitions of VA and VASP to ensure that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards;
(2) provide guidance on how the FATF Standards apply to "stable coins";
(3) provide additional guidance on the risks and potential risk mitigants for peer-to-peer transactions;
(4) provide updated guidance on the licensing and registration of VASPs;
(5) provide additional guidance for the public and private sectors on the implementation of the 'travel rule' which requires the exchanging of real name user identification during transactions; and
(6) include Principles of Information- Sharing and Co-operation amongst VASP Supervisors.

The Guidance has also been updated to reflect emerging trends over time and new requirements outlined in the publication of other relevant FATF reports.

How can Criminals Misuse Virtual Assets?

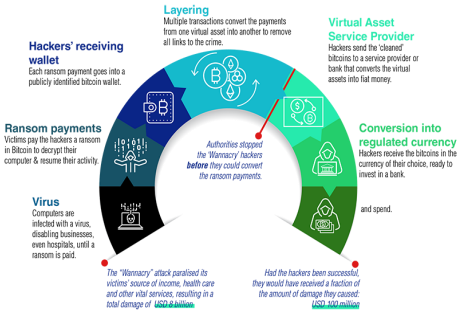
VAs have many potential benefits. They could make payments easier, faster, and cheaper and provide alternative methods for persons without access to regular financial products and services. But without proper regulation, they risk becoming a virtual safe haven for the financial transactions of criminals and terrorists.

The FATF identified potential AML/CFT risks of using VAs,

- Anonymity.;
- Lack of a centralized oversight body.;
- Global reach; and
- Complex infrastructures as the basis for the cause for concern.

Please see the FSRC's November 2020 Newsletter for more information.

In 2017, the Wannacry ransomware attack held thousands of computer systems hostage until the victims paid hackers a ransom in bitcoin. The cost of the attack went far beyond the ransom payments, it resulted in an estimated USD 8 billion in damages to hospitals, banks and businesses across the world. Other ransomware attacks have happened since and appear to be on the rise.



Closer to home, in 2020 the Caribbean's biggest conglomerate, Ansa McAl, was the victim of ransomware hackers holding some of the company's IT systems hostage. Tatil, Trinidad and Tobago's biggest insurer, was effectively stalled for about two weeks as the IT department worked to find and expel the ransomware from the Company's servers. If not, the Company would have to pay the hackers' ransom to free its data.

How do the FATF Standards Apply?

The Guidance for a Risk-Based Approach (RBA) for VAs and VASPs highlights that, "FATF Standards are intended to be technology neutral. The Guidance states that "the FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that may use these tools to facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person."

The FATF has issued guidance on requirements that countries and VASPs should implement measures to reduce risk and opportunities for criminals, terrorists and proliferation financers to launder their proceeds or finance their illicit activities.

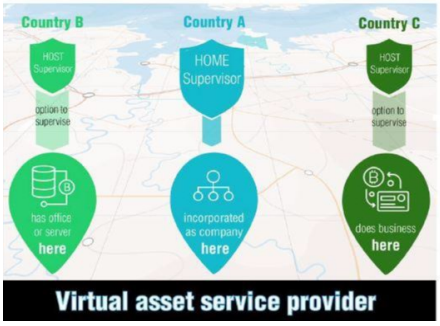
Countries need to: -

◊ Understand, identify and assess the money laundering, terrorist financing and proliferation financing risks that may arise in relation to:

(a) the development of new products and new business practices, including new delivery mechanisms; and

(b) the use of new or developing technologies for both new and preexisting products.

◊ License or register VASPs. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where the place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction.



◊ Ensure that VASPs are subject to adequate regulation and supervision or monitoring for Anti Money Laundering/ Countering the Financing of Terrorism and Counter Proliferation Financing (AML/CFT/CPF) measures and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering, terrorist financing and proliferation financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT/CPF requirements. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT/CPF requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

In 2020, St. Kitts and Nevis passed the Virtual Asset Act, No. 1 of 2020 which makes provision for the registration and regulation of virtual assets business and VASPs operating in or from St. Kitts and Nevis. In March 2021, the legislation was amended to include additional provisions for the enhancement of the regulatory framework of this sector. The legislation and related amendments can be accessed via the following link: **https://fsrc.kn/law-library/virtual-assets.**

For More Newsletters
Financial Services Regulatory Commission - Newsletters (fsrc.kn)

Virtual Asset Service Providers need to: -

◊ Implement the same preventive measures as financial institutions and Designated Non-Financial Business and Professions (DNFBPs), including customer due diligence, record keeping and reporting of suspicious transactions -

◊ Obtain, hold and securely transmit originator and beneficiary information when making transfers : The required information for each transfer includes the:

- Originator's name (i.e., the sending customer);
- Originator's account number where such an account is used to process the transaction (e.g., the virtual assets wallet);
- Originator's physical (geographical) address, national identity number or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;
- Beneficiary's name; and
- Beneficiary account number where such an account is used to

Last Note

FATF states that it is important that countries, regulators and providers recognize the cross-border and mobile nature of VAs and the VASP sector. Effective regulation, supervision and enforcement of this burgeoning sector requires a global approach and international co-operation.

International co-operation is also relevant in the context of VASPs that seek to register or license themselves in one jurisdiction but provide products or services "offshore" to customers located in other jurisdictions.

In this Newsletter……..

REFERENCES

CFATF Guidance Document: How can Virtual Assets be used for the Commission of Financial Crimes— 24 March 2021

LexisNexis White Paper: A Risk-Based Approach to Virtual Assets and Virtual Asset Providers—December 2019

Guidance for a Risk Based Approach for VAs and VASPs—June 2019

FATF Report—Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing —September 2020