EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

Public Summary

REPORT ON ABUSE OF VIRTUAL ASSETS FOR TERRORIST FINANCING PURPOSES

Information Exchange Working Group (IEWG)

June 2023

Table of Contents

ABBREVIATIONS

FIU	Financial Intelligence Unit
VA	Virtual Asset
IEWG	Information Exchange Working Group
FATF	Financial Action Task Force
VASP's	Virtual Asset Service Providers
Peer2Peer	Distributed application that partitions tasks or workloads between peers
TF	Terrorism Financing
CFT	Countering Terrorism Financing
AML	Anti-Money Laundering
ISIL	Islamic State of Iraq and the Levant
FININT	Financial Intelligence
IP	Internet Protocol
MSB's	Money Service Businesses
FIS	Financial Institutions
DNFBP	Designated Non-Financial Businesses and Professions
FTF	Foreign Terrorist Fighter
PF	Proliferation Financing
LEA	Law Enforcement Agency
KYC	Know Your Customer
STR	Suspicious Transaction Report
ATM	Automated Teller Machine

CAD	Canadian Dollar
TOR	Onion Rooter
I2P	Invisible Internet Project
CASP	Crypto Asset Service Provider
EU	European Union
NCBTF	National Bureau for Counter Terror Financing Israel
IMPA	Israel Money Laundering and Terrorist Financing Prohibition Authority
ESW	Egmont Secure Web
BTC	Bitcoin
CDD	Customer Due Diligence
OSINT	Open-Source Intelligence
IP	Internet Protocol
SAR	Suspicious Activity Report
RMVE	Religiously Motivated Violent Extremist
DEFI	Decentralised Finance Platforms
NFT's	Non-Fungible Tokens
ECOFEL	Egmont Centre of FIU Excellence and Leadership
TATWG	Technical Assistance and Training Working Group

1. Introduction

As an organization of FIUs, the Egmont Group (EG) is conscious that Virtual Assets (VAs) abused in terrorism financing is a current focal point of discussions at fora. Understanding trends in emerging technologies will aid in the identification of potential vulnerabilities associated with new technologies, specifically VAs. They can be instantly traded through peer2peer platforms, for example, and transferred on the Internet, which is generally characterized by non-face-to-face customer relationships and may permit anonymous funding. In addition, it is well-known that terrorist organizations and individual terrorists are trying to work in full conspiracy, which makes VAs a natural target for facilitating their financial activities.

The IEWG project on the *Abuse of Virtual Assets for Terrorist Financing Purposes* was designed to assess the exposure to possible abuse, as well as to record the best practices that are used by EG member FIUs to prevent the abuse of virtual assets for terrorist financing purposes.

The project's key objectives were to explore the abuse of VAs for TF, by:

- Understanding the regulation of VAs in different countries,
- Identify how VAs are defined in different countries,
- Determine VA usage and detection,
- Develop a framework, standard or best practices document for the use by FIUs, and
- Sharing of case studies.

EG member FIUs are well-positioned to identify and trace suspicious transactions, activities, individuals, and entities. However, as previously identified in other Egmont Group reports (Lone Actors and Small Cells), FIUs usually face difficulties with TF cases, especially when they are excluded from the domestic (CFT) apparatus, when they are not appropriately empowered or provided with the necessary technical and analytical capacity to produce financial intelligence effectively, or when information is generally missing for specific financial or other services. This could be the case with VAs, where although jurisdictions are obliged by the Financial Action Task Force (FATF) Standards to collect and possess information regarding Virtual Asset Service Providers (VASPs') activities on their territory and apply the FATF "travel rule,"[1] many remain under the radar of the competent domestic authorities engaged with the registration and/or licensing of VASPs.

2. Literature Review

Several research papers reflect on how VA presents a huge AML/CFT risk to the integrity of the financial system. The Egmont Group itself has previously dedicated resources to examine the topics of TF through the ISIL Project and Vas through the development of the e-Catalogue on regulated VASPs. In addition, the FATF and the IMF have produced public reports that examine the abuse of VAs.

FATF work:

2020 FATF Report Virtual Assets Red Flag Indicators

In October 2018, the FATF updated its Standards to clarify the application of the FATF Standards to VA activities and VASPs. The updates assisted jurisdictions in mitigating the money laundering and terrorist financing (ML/TF) risks associated with VA activities and in protecting the integrity of the global financial system. In June 2019, the FATF adopted an *Interpretative Note to Recommendation 15* to further clarify the application of FATF requirements to VA activities or operations and VASPs, including with respect to suspicious transaction reporting.

The *2020 FATF Virtual Assets Red Flag Indicators Report* [2]provided a practical tool for both the public and private sectors in identifying, detecting, and ultimately preventing criminal, ML, and TF activities involving VAs. The report provided ML/TF red flag indicators associated with VAs to assist reporting entities, including financial institutions (FIs), designated non-financial businesses and professions

[1] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

[2] https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

(DNFBPs), and VASPs. The indications (or any single sign) should not be considered in isolation because they are frequently just one of many components that go into a larger overall picture of possible ML or TF risk. Therefore, it is recommended that competent authorities distribute this study to reporting entities and hold engagement and awareness-raising workshops with them to help them better comprehend it. Competent authorities may also provide private sectors with the indicators and information most relevant for that jurisdiction.

IMF Work:

2021 Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2) Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework— Some Legal and Practical Considerations

The 2018 and 2019 revisions to the standards provided much-needed clarification on how VASP regulation and supervision should be carried out. This has been crucial for establishing greater uniformity among jurisdictions' strategies for reducing the risks to VAs' financial integrity and preventing regulatory arbitrage. The FATF has ensured that the new actors in the virtual environment are treated properly and that comparable risks are addressed equitably by subjecting VASPs to measures identical to those already applicable to FIs and DNFBPs.

The likelihood of the VASPs Interacting with the traditional financial sector, including the banking sector, has also increased. Several VASPs have stated that the advantages of implementing reliable AML/CFT systems outweigh the drawbacks, particularly because it has given banks confidence that the ML/TF/PF risks were sufficiently mitigated to allow them to conduct banking activities.

The 2021 paper[3] offered recommendations to make it possible to comprehend and reduce the financial integrity issues that VAs pose. The first Fintech note clarified which assets and service providers should be subject to AML/CFT measures, the steps that all jurisdictions should take, the kind of action required in cases of criminal misuse of VAs, and the reasons why VAs are vulnerable to misuse for ML/TF/financing the proliferation of weapons of mass destruction (PF).

The second Fintech note focused on the AML/CFT regulation and supervision of VASPs. It expanded on Fintech Note 1 and aimed to give competent authorities and policymakers a high-level overview of the AML/CFT regulatory and supervisory frameworks planned for VA and VASPs, as well as some of the practical and legal concerns they bring.

3. Methodology

To achieve the project objectives, the project team relied on existing literature and new information collection through a tailor-made questionnaire. The survey/questionnaire was circulated, and FIUs provided their respective responses. From the responses received, a report was drafted that included several case studies on the abuse of VAs for TF, which highlights several key risks and best practices on the abuse of VAs for TF purposes. However, these case studies are not included in this sanitized version of the report.

[3] https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-2-463657

It is the understanding of the project team that the collected data represents a sufficient level of regional diversity and generally reflects the amount of information collected within other CFT-related projects.

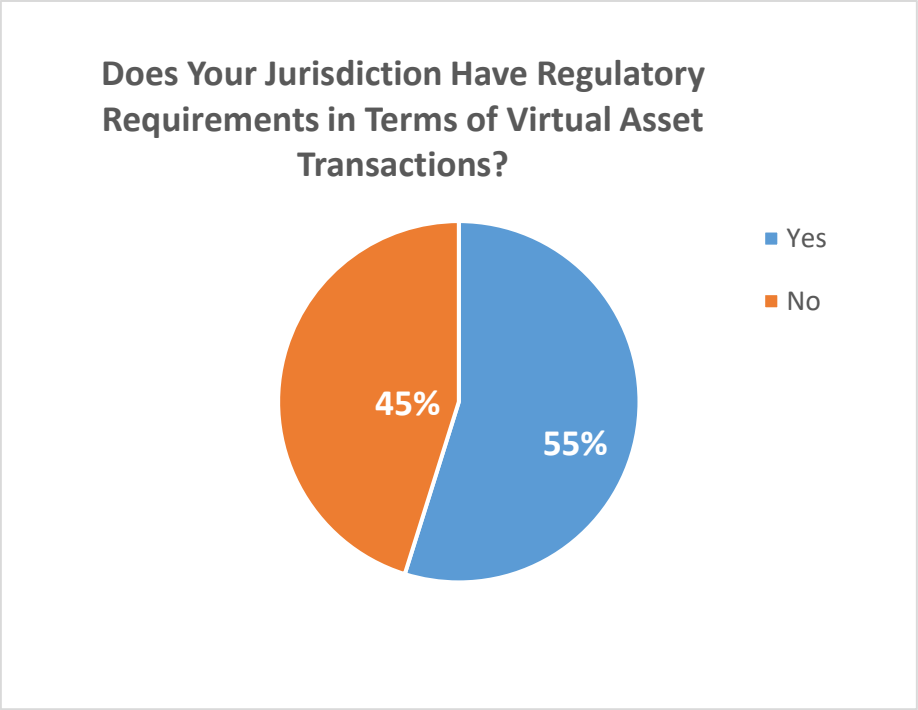
This IEWG report serves as a guide to understanding new trends and the sharing of best practices in emerging technologies that will aid towards the identification of potential vulnerabilities associated with VAs.

In that sense, the conclusions provided in the last chapter of the report could be instrumental for FIUs' attempts to tackle TF through VAs.

4. Technology and Compliance

4.1 Regulatory Requirements in Terms of Virtual Asset Transactions

In this section of the document, the necessary regulatory requirements concerning virtual asset transactions in their respective jurisdictions were analyzed.



Of the total **FIUs that replied** to this question, our analysis shows that:

- **55% of FIUs** state that their jurisdictions have regulatory requirements in terms of VA transactions.
- **45% of FIUs** state that their jurisdictions do not have regulatory requirements in terms of VA transactions.

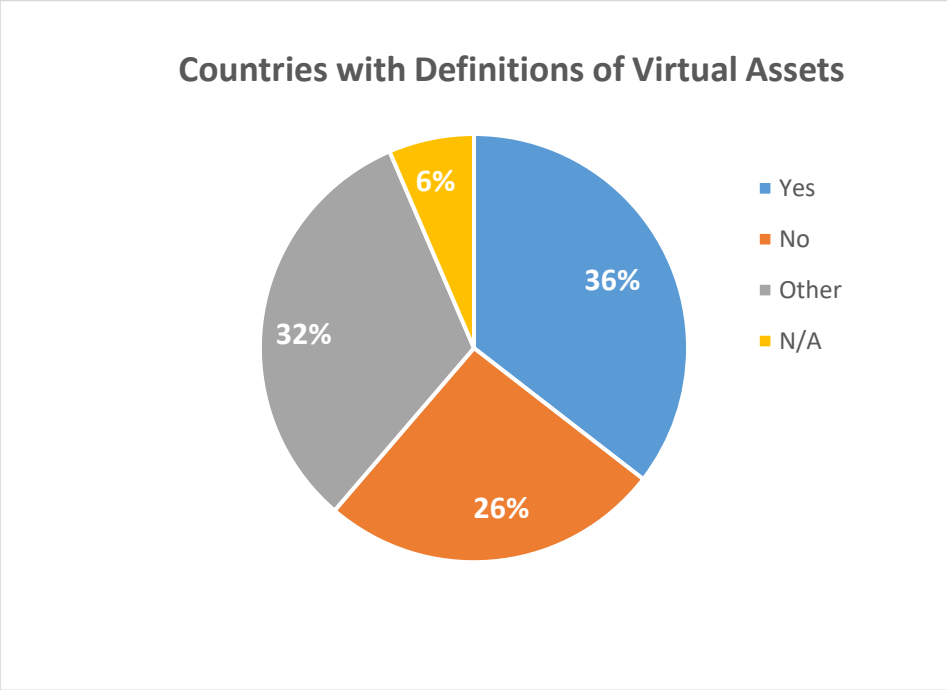
Although the FATF amendments in R.15, introducing requirements regarding transactions and services with VAs, were adopted back in October 2018, around 45% of the responding FIUs are still not regulating them. This shows the need for such regulation, which would allow competent authorities to collect relevant data and apply direct risk-mitigation measures.

4.1.1 Restrictions, Disclosures, or Regulatory Compliance Requirements

Out of the **55% FIUs** that stated that their jurisdictions have regulatory requirements in terms of VA transactions, all of them answered this question and shared some restrictions, disclosures, or regulatory compliance requirements applicable to virtual asset transactions to their jurisdiction, such as:

- Complying with AML/CFT laws and measures set by their jurisdictions.
- Following regulatory standards comparable to those applicable to licensed FIs.
- Proceeding to a proper assessment of Know Your Customer (KYC) procedures.
- Identifying the origin of funds and the beneficiary of transactions.
- Understanding and monitoring business relationships.
- Gathering information on whether a person is a politically exposed person.
- Reporting suspicious transactions (STR).

4.1.2 Virtual Assets Defined



Amongst the participating FIUs, our analysis shows that:

- **36% of FIUs** have a clear definition of VA.
- **26% of FIUs** do not have any definitions regarding VA.
- **6% of FIUs** unfortunately did not provide a reply to the question.
- **32% of FIUs** gave alternative definitions of VA.

The results of this question show that there might be a gap in the proper understanding of what VAs are and which of them should be precisely regulated. This may lead to gaps in the overall reporting.

5. Encrypted Networks (Dark Web)

5.1 Use of Virtual Assets in Illicit Markets

Most FIUs who provided an answer to this specific question have significant experience in identifying the use of virtual assets in illicit markets (dark web). 16% of FIUs indicated not having information on the widespread use of virtual assets in illicit markets in their jurisdiction. However, the potential use of VAs as a tool to finance illicit activities is acknowledged well. One FIU noted that virtual assets as such are illegal in their corresponding jurisdiction.

In general, most FIUs have experience in identified use of virtual assets in illicit markets. Several FIUs regularly receive suspicious transaction reports related to the activity involving the use of virtual assets in the darknet. Investigations have led to particular darknet platforms where the common payment method includes cryptocurrency, the most popular being Bitcoin.

6. Virtual Currency Usage and Terrorist Financing Detection

6.1 Detecting and Analyzing Financial Transactions

Under the challenges related to the investigation process, there is a noted difficulty in identifying VASPs and obtaining KYC information.

In 2015, FATF expanded the risk-based approach to include operations involving virtual assets in its guidance. In 2018, the FATF amended Recommendation 15, extending AML standards to crypto businesses, including exchanges and wallet providers.

In 2019, the FATF updated its recommendations on virtual assets and issued an Interpretive Note to Recommendation 15. The documents addressed the definition of virtual assets service providers and their AML requirements, including customer due diligence, KYC, recordkeeping, transaction monitoring, suspicious transaction reporting, and applying the risk-based approach.

There is a need for strong international cooperation with partner FIUs, as mentioned by some of the FIUs, especially in cases where the VASP is registered in another jurisdiction. Cooperation with the INTERPOL and with the overseas LEAs was also noted for a better understanding of the asset recovery system and of legal frameworks in different jurisdictions.

Some of the FIUs indicated the need to enhance the legal framework to include the VAs. A small group of FIUs noted the plan to introduce a licencing regime for VASPs and subject them to a fit-and-proper test similar to that of other financial sectors.

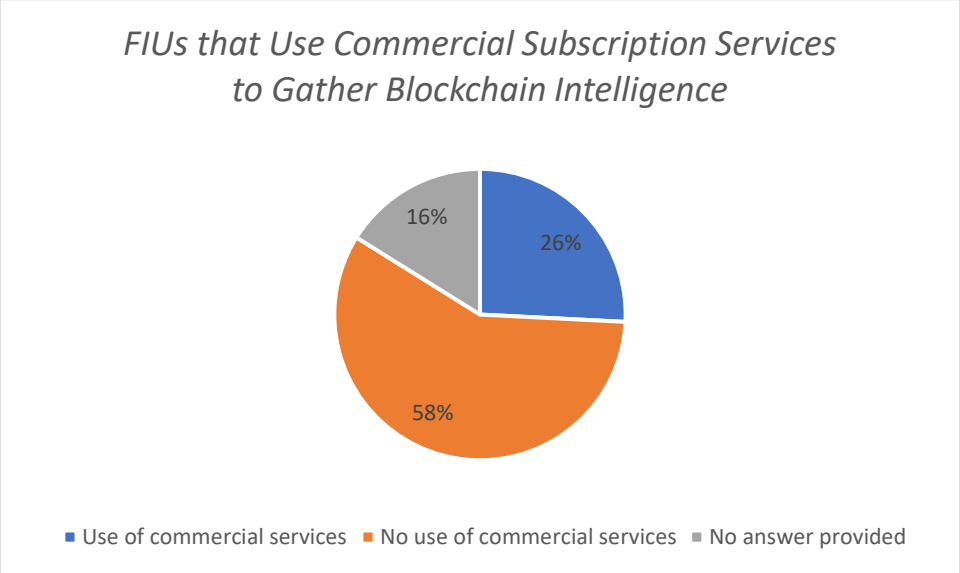
7. Virtual Currency Usage and TF detection.

7.1 Challenges, Lessons Learned and Best Practices for FIUs

7.1.1 Use of Commercial Subscription Services to Gather Blockchain Intelligence

Many tools are available on the market to collect information on blockchain and to link wallets, virtual assets, and other technical data with a potential criminal user.

These various tools can be used by FIUs to improve their analyses as they provide tracing possibilities of transactions with VAs.



7.1.2 Determining Red Flag Indicators

As is the case in the traditional financial system, it is possible to observe certain potentially suspicious behaviour in the context of transactions that take place with Virtual Assets. Each suspicion concerning a transaction, an attempted transaction or knowledge of a fact in the customer's domain, must prompt the obliged entity to send an STR/SAR to the FIU.

To detect a potentially suspicious transaction, red flags can be used to cover many possible scenarios. These indicators can be used within transaction monitoring tools to automatically highlight any potential suspicious transactions.

However, to avoid having too much information to analyze that would turn out to be irrelevant, it is necessary to have red flag indicators that are as precise as possible and adapted to different scenarios. The idea is to have the lowest possible number of false positives. The red flag indicators must therefore act as a first filter to select certain potentially suspicious transactions.

The potentially suspicious transactions highlighted by the indicators combined with facts or additional elements obtained during the analysis of the client make it possible to determine whether there are sufficiently reasonable grounds to suspect that the transaction was carried out to commit or attempt to commit an ML/FT offence. A red flag indicator may not, on its own, be sufficient to determine whether an operation or transaction is truly suspicious.

In the context of cryptocurrencies, indicators relating to the financing of terrorism can be established. However, the difficulty lies in the fact that these indicators can sometimes be the same as those used to detect suspicious transactions in the context of money laundering.

Some red flag indicators can be more oriented in cases of terrorist financing, and some are part of a much broader context and can be linked to suspicions of money laundering as well as terrorist financing. The contribution of additional elements, in particular related to knowing the customer (KYC), is, therefore, all the more important to determine the suspicious nature of the transaction in the context of the financing of terrorism.

Geographical risks associated with exchange transactions usually take place via digital asset exchanges or brokers. The choice of digital asset exchanges and brokers for an exchange transaction should not be underestimated.

It was also noted from recent statements by a jihadist group that they have discontinued using VAs for fundraising purposes due to the "successful government efforts to identify and prosecute donors".

7.1.3 Modus Operandi Linked to Groups or Individuals

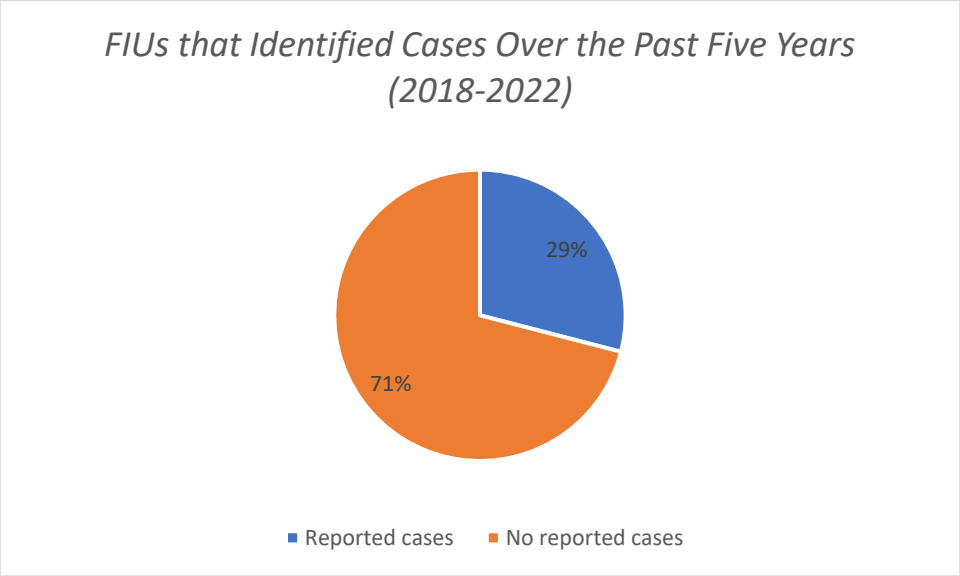
In general, in the context of terrorist financing, the difficulty of detection lies in the fact that the amounts transferred are often small and that this financing is not often directly linked to an individual or group involved in terrorism.

Due to this indirect nature of funding, the funds transferred through Virtual Assets can therefore move from one virtual address to another without being detected.

7.2 Identified Cases by the FIU Over the Past Five Years (2018-2022)

Of the FIUs that took part in the survey:

- 29% of the respondents have identified cases in which Virtual Assets were linked to terrorism financing.
- 71% of the respondents did not report any cases.



7.3 Identified Terrorist Organizations

Among the various FIUs that have been able to identify cases where Virtual Assets were used to conduct terrorist financing activities, different types of organisations (domestic or international) were found to be involved.

Most of the time, donors or supporters were identified as sending funds to individual or group addresses linked to terrorist organizations present in conflict zones, such as ISIL, Al-Qaeda, and other extremist groups, such as Hamas and the Al-Qassam Brigades.

Other cases concerned the sending of funds directly to cryptocurrency exchange platforms located in the Middle East having links to TF.

FIUs also observed the abuse of VA by individuals who support right-wing organizations and individuals known to be rooted in radical religious behaviour.

All the aforementioned information suggests that terrorist organizations and groups deliberately misuse VAs for their purposes.

8. Conclusion

Based on the above study, it is clear that VAs pose a potential threat for ML/TF. Understanding trends and sharing of best practices in emerging technologies will aid in the identification of potential vulnerabilities associated with new technologies.

While a limited number of FIUs submitted replies and case studies, the collected data represents a sufficient level of regional diversity. A majority of responding FIUs indicated that they have regulatory requirements regarding VA transactions, and it is compulsory to comply with the anti-money laundering and countering the financing of terrorism laws and measures set by their jurisdictions. Although the FATF amendments in R.15 introduced requirements regarding transactions and services with VAs in October 2018, a significant portion of the responding FIUs are still not regulating it.

Due to the nature of the VAs, they currently cannot be widely used for purchasing goods or services and, therefore, cannot provide an optimal capacity to serve as a medium of exchange. This is also important in TF cases because most terrorists are deprived of using their assets due to sanctions regimes or of keeping their criminal conspiracy. Therefore, for terrorists and their financiers, it would be of profound importance to be able to transform VAs into fiat currency anonymously and vice versa.

In general, most FIUs have experience in identifying the use of VA in illicit markets. Several FIUs regularly receive suspicious transaction reports related to the activity involving the use of Virtual Assets in the darknet.

Challenges include raising awareness of obliged entities and receiving STRs on VAs. In addition, FIUs mentioned that none of the STRs they have received involving VAs incorporate a TF aspect. There is a need for strong international cooperation with partner FIUs, especially in cases where the VASP is registered in another jurisdiction.