Guidance on identifying, assessing and understanding Terrorist Financing Risks in the context of Crypto Assets activities

01 June 2023

CONTENTS

A. INTRODUCTION

This document was prepared to provide guidance for the Regulated Entities of the Cyprus Securities and Exchange Commission ("the CySEC") to identify, assess and understand the Terrorist Financing ("TF") risks in relation to Crypto Asset activities, in order to implement adequate and appropriate policies, controls and procedures so as to mitigate and manage those risks effectively.

Characteristics associated with these assets can be exploited by terrorists and criminals to finance illicit activities. Therefore, it is important that the Regulated Entities ensure that they can adequately identify and understand the risks they face, so as to effectively implement a risk based approach of counter TF measures.

Information contained in this guidance is not supposed to be exhaustive, but rather to provide helpful considerations for CySEC's Regulated Entities to identify, assess and understand the TF risk. This guidance recognises that there is no one-size fits all approach when identifying and assessing TF risk and Regulated Entities will need to extract from this guidance those parts that are most relevant to their unique context and threat profile. Regulated Entities are responsible for designing policies and measures to address TF risks based on the existing regulatory framework.

This guidance document is meant to be read in conjunction to the relevant legislation and any other relevant guidance issued by CySEC on these issues, such as:

- **Policy Statement PS-01-2021** - on the Registration and Operations of Crypto-Asset Service Providers.
- **Circular C276** - The Application of the Risk Factors Guidelines.
- **Circular C299** - Guidance on Identifying, Assessing and Understanding the Risk of Terrorist Financing in Financial Centres.
- **Circular C339** - Financial Action Task Force (FATF) Guidance on Terrorist Financing Risk Assessment.
- **Circular C432** - Opinion of the European Banking Authority on the risks of Money Laundering and Terrorist Financing affecting the European Union's financial sector.
- **Circular C465** - Revised EBA Guidelines on ML/TF risk factors.
- **Circular C476** - Financial Action Task Force (FATF) Guidance on Risk-based Approach for Virtual Assets and Virtual Asset Service Providers.
- **Circular C478** - National Risk Assessment on Money Laundering and Terrorist Financing Risks with respect to Virtual Asset and Virtual Asset Service Providers.
- **Circular C550**- Common weaknesses/deficiencies and good practices identified during the onsite inspections performed in relation to the prevention of money laundering and terrorist financing.
- **Circular C535** - EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849.
- **Circular C556** - Guidance on Sanctions and Restrictive Measures

B. CYPRUS REGULATORY FRAMEWORK

Cyprus has transposed the 5th EU Anti Money Laundering Directive (AMLD5) into its national law, through amending Law 188(I)/2007 on the Prevention and Suppression of Money Laundering and Terrorist Financing ("the AML/CFT Law"). On 23 February 2021, the amendment of the money laundering regulations became effective and Crypto Asset Service Providers ("CASPs") became obliged entities for anti-money laundering purposes. In the context of transposing the relevant provisions of AMLD5 into national Law, the following crypto-asset's activities are also included under the AML/CFT obligations (which were not included in the AMLD5):

i. exchange between crypto-assets;
ii. transfer of crypto-assets;
iii. participation in and provision of financial services related to an issuer's offer and/or sale of a crypto-asset.

According to Section 59(1)(b)(vii) of the AML/CFT Law, CySEC was designated as the competent authority in relation to registered providers of services concerning crypto-assets provisioned under Section 61E of the AML/CFT Law.

Furthermore, on 21 May 2019, the Combating of Terrorism and Victims' Protection Law N. 75(I)/2019 was published in the official gazette and the CySEC engages as part of its supervisory activity with a view to discharging its supervisory responsibilities under this law. The Combating of Terrorism and Victims' Protection Law deals with a number of issues, including the definition of terrorism felonies, the responsibilities of legal persons, responsibility of entities obliged under the AML/CFT Law to confiscate property belonging or controlled by persons engaged in terrorism and the responsibility of supervisory authorities for ensuring that obliged entities abide with the relevant provisions of this law.

In addition, CySEC issued a new Directive (secondary legislation) in relation to the registration of CASPs, the CASPs Registration Directive, which came into force on 25 June 2021.

On 13 September 2021, CySEC published a Policy Statement on the registration and operations of CASPs. The terms 'Crypto-asset' and 'Crypto Asset Service Providers' are both defined in the AML/CFT Law and CySEC's Policy Statement on the Registration and Operations of Crypto-Asset Services Providers (PS-01-2021).

Thus, the applicable regulatory framework for CASPs, is now comprised of:

- The AML/CFT Law;
- The CASP Registration Directive;
- The CySEC Directive for the prevention and suppression of Money Laundering and Terrorist Financing.

A designated section was created on the CySEC's website that includes all the information mentioned above.

CASPs, within the meaning of the Prevention and Suppression of Money Laundering and Terrorist Financing Law ("AML/CFT Law"), must formally register with the Cyprus Securities and Exchange Commission ("CySEC"). CASPs registered with CySEC are obliged entities under the AML/CFT Law and hence they must fully abide to their obligations stemming from the relevant regulatory framework and relevant Guidance issued by CySEC.

According to the Article 58 (d) of the AML/CFT Law, Regulated Entities should apply adequate and appropriate policies, controls and procedures which are proportionate to their nature and size, so as to mitigate and manage the risks of Money Laundering ("ML") and TF effectively, in relation to internal control, risk assessment and risk management in order to prevent ML and TF. Specifically, the Article 58(A) of AML/CFT Law, notes that the Regulated Entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing which it faces, taking into account risk factors, including among others, factors which relate to its customers,

countries and geographical areas, provided that such measures are proportionate to the nature and size of the Regulated Entity.

The Regulated Entities must be able to demonstrate to CySEC that the particular degree of measures is appropriate in view of the risks of TF to which they are exposed. Also, for the development of the risk-based approach, Regulated Entities are advised to consider the EBA's Risk Factor Guidelines. This approach involves conducting a risk assessment that considers the specific risks associated with their business activities, customer base and geographic location, among other factors. Regulated Entities are required to assess the risk inherent in their business taking a holistic approach and considering all the factors to which they are exposed. Regulated Entities are expected to identify the areas that pose higher risks and apply enhanced measures accordingly.

C. FATF GUIDANCE AND EBA GUIDELINES

FATF Guidance

Regulated Entities are urged to consult, inter alia, FATF publications. The Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog that has set global standards to prevent these activities, has paid particular attention to the crypto-assets sector, issuing the below reports/public statements:

Virtual Currencies: Key Definitions and Potential AML/CFT Risks, published in June 2014.

Guidance for a Risk-Based Approach to Virtual Currencies, published in June 2015.

Guidance for a Risk-Based Approach for Virtual Assets and VASPs, published in June 2019.

The "FATF INR 15 Interpretative Note", published in June 2019

12-month review of the Revised FATF Standards on VAs and VASPs, published in June 2020.

Report to the G20 on So-called stablecoins, published in June 2020.

VA Red Flag Indicators for ML/TF for use by the public and private sectors, published in September 2020.

Guidance on a Risk-based approach to AML/CFT supervision, published in March 2021.

Second 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs, published in July 2021.

Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, published in June 2022.

EBA Guidelines

On 12 August 2021, CySEC issued Circular C465 for the implementation of European Banking Authority Guidelines (EBA/GL/2022/05) in order to inform the Regulated Entities of the Revised EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering (ML) and terrorist financing (TF) risk associated with individual business relationships and occasional transactions. The EBA emphasizes that the non-exhaustive list of risk factors on TF was included following feedback of the industry during the public consultation of the first version of the Risk Factors Guidelines. CySEC called upon the Regulated Entities to comply with the Guidelines and be able to establish sound policies, controls and procedures.

According to the EBA guidelines, Regulated Entities are required to assess the TF risk inherent in their business, taking into consideration relevant factors, such as their customers and the geographical areas to which they are exposed. Amongst others, these include:

- **Customer risk factors**

  When identifying the risk associated with a customer or beneficial owner's nature and behaviour, firms should pay particular attention to risk factors that, although not specific to TF, could point to increased TF risk, in particular in situations where other TF risk factors are also present. To this end, firms should consider at least the following risk factors:

  a. Is the customer or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures ,or are they known to have close personal or

professional links to persons registered on such lists (for example, because they are in a relationship or otherwise live with such a person)?

b. Is the customer or the beneficial owner a person who is publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity, or are they known to have close personal or professional links to such a person (for example, because they are in a relationship or otherwise live with such a person)?

c. Does the customer carry out transactions that are characterised by incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offences are known to be operating, that are known to be sources of TF or that are subject to international sanctions? If so, can these transfers be explained easily through, for example, family ties or commercial relationships?

d. Is the customer a non-profit organization

   i. whose activities or leadership been publicly known to be associated with extremism or terrorist sympathies? Or

   ii. whose transaction behaviour is characterized by bulk transfers of large amounts of funds to jurisdictions associated with higher ML/TF riks and high-risk third countries?

e. Does the customer carry out transactions characterized by large flows of money in a short period of time, involving non-profit organizations with unclear links (e.g. they are domiciled at the same physical location; they share the same representatives or employees or they hold multiple accounts under the same names)?

f. Does the customer transfer or intend to transfer funds to persons referred to in (a) and (b)?

❖ **Countries and Geographical areas**

When identifying the level of TF risk associated with a jurisdiction the following risk factors should be considered:

a. Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities, either from official sources or from organized groups or organizations within that jurisdiction?

b. Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that groups committing terrorist offences are known to be operating in the country or territory?

c. Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?

D. TF RISKS IN THE CONTEXT OF CRYPTO-ASSETS AND CASPs OPERATIONS

According to Article 2 of the AML/CFT Law, **'Terrorism Financing'** is defined as the provision or gathering of funds by any means, directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part for the commission of an offence. Regulated Entities should refer to the meaning given to the term by section 4 of the International Convention for the Suppression of the Financing of Terrorism (Ratification and Other Provisions) Law and by sections 5 to 13 of the Combating of Terrorism Law.

Differences between TF and ML

Although ML and TF have similarities, they have important differences which must be understood in order to distinguish suspicious terrorist financial activity from ML.

The most important difference involves the origin of funds, thus TF funds are not necessarily illegally obtained, they are often clean legal funds to commit a crime. ML involves funds derived from illicit proceeds with the purpose of using them to perform legitimate activities. Also, TF uses

small amounts and transactions involving unrelated parties as opposed to ML activity which involves large amounts of money.

Tracing money differs between TF and ML; in the case of TF money is used to fund TF activities by many and, in many cases, unrelated to the initiator whereas in the case of ML the funds are eventually transferred to the person (s) who initiated the proceedings.

Crypto-Assets specific TF vulnerabilities and risks

Like other financial products and services, crypto-assets have features that present risks for facilitating criminality, including TF. When it comes to the consideration of the product/service/transaction risk, it is expected that Regulated Entities will take into account the particular nature of crypto-assets as well as the underlying and associated technologies that can impact the TF risk arising from them.

Advances in technology and the use of crypto-assets for payments have characteristics and certain features that may be attractive to terrorists and a broader range of extremist actors (Dion- Schwarz et al., 2019; Europol, 2022; Information Exchange Working Group, 2022; Schwarz Nadine et al., 2021).

Some illustrative examples are presented below:

- The use of crypto-assets enables greater anonymity than traditional funding channels;
- Certain digital wallets and privacy may be used which enable data anonymization;
- There is the possibility of anonymous funding if the sender and the recipient are not identified properly or if cryptocurrency mixers and tumbler services and enhanced cryptography are used to obscure the financial audit of the transactions;
- Users can receive payments from unknown sources worldwide;
- Cheaper and faster cross-border payments as crypto-assets can be quickly used for large-scale cross-border transactions;
- Customers are mostly non-face-to-face;
- They can provide links to dark net marketplaces where they can be accepted as a method of payment;

- Decentralization - Terrorists can use cryptocurrencies owing to the perceived advantages of decentralization. Because they are open-source, decentralized applications, cryptocurrencies are often described as 'permissionless'; that is, access to them cannot be restricted and users may transfer their crypto-assets without the involvement of a CASP (peer-to-peer ("P2P") transactions), thus bypassing AML/CFT obligations, such as the FATF's travel rule;
- P2P transactions allow users to send crypto-assets to beneficiaries regardless of geographic boundaries, as long as the beneficiaries have a virtual asset address and an internet connection;
- The existence of gaps in the implementation of international AML/CFT standards in different countries, especially in jurisdictions where AML/CFT standards for crypto-assets are lacking or poorly enforced;
- CASPs that do not comply with AML/CFT requirements and other regulatory obligations;
- The use of platforms that allow for the conversion from one asset to another without these transactions being recorded in the blockchain;
- The use of emerging technology that allows the parties to send and receive crypto-assets without needing each transaction to be recorded on the blockchain.

These are not the only potential risk factors relevant to the CASPs business and should not be the only risks considered in the risk assessment – they are however important overarching themes relevant to the CASP sector. Key vulnerabilities and high-risk factors relevant to CASPs business do not operate in isolation but in combination, resulting in a compounding risk of TF.

Overall, combined with other crypto asset characteristics such as privacy can provide terrorists with the cover they need to conduct transactions and launder proceeds of crime when such activity goes undetected.

International evidence

Despite the low number of Suspicious Activity Reports and Suspicious Transaction Reports (SARs/STRs) related to crypto-assets, various analyses confirm that the TF risk with regard to crypto-assets does exist. Global evidence shows that the use of crypto-assets has not replaced

traditional TF methods as criminals tend to use pre-existing financial services for TF. However, the use of crypto-assets or CASPs to support TF have emerged as a channel (Europol 2022, Information Exchange Working Group 2022). The role of new technology in TF was highlighted by the FATF in October 2015 in its report on 'Emerging Terrorist Financing Risks'.

Several cases showed the potential of crypto-assets in terrorism financing and several recent examples of fundraising by terrorist groups illustrate this. Evidence shows that some terrorist groups and their supporters are now more familiar with new technologies as a source of finance (Salami 2017, Hanley 2020). The use of crypto-assets by terrorist organizations is also documented. Several organisations have made calls for donations through social networks, forums or private groups, disseminating crypto-assets addresses to which funds are sent to finance their criminal activities (Chainalysis 2023, Elliptic 2022, Ciphertrace 2022). It is possible that, terrorist groups will further diversify their strategies in both expected and unexpected ways in terms of funding sources and use of funds. Terrorists are using this technology with greater sophistication, the situation is dynamic and the potential danger is significant (European Commission, 2022).

Evidence from Cyprus

The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) during its last evaluation report observed that, while the terrorism threat was considered to be low in Cyprus, the authorities rated TF risk as medium due to the country being an International Financial Centre and its proximity to conflict areas (Moneyval, 2019). According to a US State Department report for Cyprus published in 2020, there were no terrorist incidents in Cyprus in 2020. Furthermore, this report noted the termination of the Cypriot investment programme eliminated a potential source of TF risk (Department of State, 2020).

There are no local groups recognized as terrorists in Cyprus. It is assumed that the TF threat from external finance is higher than the threat from domestic finance. There is no evidence that Cyprus CASPs are significantly exposed to TF and the use of crypto-assets in the Island is still low. To

illustrate, on the ranking list for the world index of adoption of cryptocurrencies for 2022 as prepared by Chainalysis, Cyprus is ranked 110th out of 146 countries (Chainalysis, 2022). As of 31 December 2022, Cyprus counts only seven (7) registered CASPs. Also the uses of blockchain technology in Cyprus is still limited (Georgiou, 2021).

However, according to the FATF report "Terrorist Financing Risk Assessment Guidance":

"It is important that countries assess and continue to monitor their TF risks regardless of the absence of known threats. The absence of known or suspected terrorism and TF cases does not necessarily mean that a jurisdiction has a low TF risk. In particular, the absence of cases does not eliminate the potential for funds or other assets to be raised and used domestically (for a purpose other than terrorist attack) or to be transferred abroad. Jurisdictions without TF and terrorism cases will still need to consider the likelihood of terrorist funds being raised domestically (including through willing or defrauded donors), the likelihood of transfer of funds and other assets through, or out of, the country in support of terrorism, and the use of funds for reasons other than a domestic terrorist attack".

Despite the low evidence of TF and the low number of terrorist-related transactions to date in Cyprus, the risks related to TF cannot be ignored. Cyprus is a financial centre that has a volume of cross-border assets being managed and transferred. On February 28 2019, CySEC issued Circular C299 to inform the Regulated Entities on the Guidance on Identifying, Assessing and Understanding the Risk of TF in Financial Centres issued by Moneyval.

As with many other countries, terrorist threats to Cyprus may come from neighbouring countries. In addition, the fact that the island is divided precludes cooperation between the Republic of Cyprus, the occupied territories and Turkey to combat terrorism financing (Cyprus AML Advisory Authority, 2021). The risk of a future use of Cypriot CASPs by terrorists to transact in crypto-assets either through donations or by selling illicit goods cannot be ignored.

E. IMPLEMENTATION PROCEDURES

Identifying and Assessing terrorist financing risk -Risk Based approach

Considering the Article 58(d) of the AML/CFT Law, Regulated Entities should apply appropriate policies, controls and procedures among others in relation to risk assessment and risk management so as to mitigate and manage the risks of terrorist financing effectively.

Specifically, the Article 58(A) of AML/CFT Law, notes that the Regulated Entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing which they face, taking into account risk factors, including among others, factors which relate to their customers, countries and geographical areas, provided that such measures are proportionate to the nature and size of the Regulated Entity.

Customer Due Diligence

Article 58(a) of the AML/CFT Law, provides the requirements for undertaking customer due diligence. Regulated Entities should conduct customer identification and due diligence procedures to identify and verify the customer and ensure that they are not dealing with individuals or entities that are associated with TF.

In addition to carrying out customer due diligence measures, under the Article 60 of the AML/CFT Law, customer due diligence measures, among others, should also be carried out when there is a suspicion of TF. In these cases, customer identification and due diligence procedures should be applied regardless of the amount or any derogation, exemption or minimum threshold pursuant to the provisions of the Law.

Enhanced Customer Due diligence

The extent to which the customer due diligence measures are applied may vary based on the risk identified. Specifically enhanced due diligence measures should be applied in situations presenting a high risk of TF. In this regard, considering Article 64(3) of the AML/CFT Law, when assessing the said risk, Regulated Entities have to take into consideration the non-exhaustive list of factors and types of evidence of potentially higher risk included in **Annex III** of the AML Law.

Transaction monitoring

The Regulated Entities should apply procedures and controls so as to mitigate and manage the risk of terrorist financing in relation to the transactions following the details of the Article 58(e) of the AML/CFT Law.

Especially for transaction monitoring and Customer Due Diligence, Regulated Entities can benefit from widely available tools. Transactional analysis tools using blockchain technologies allow transactions and crypto-assets to be traced. Such tools are essential components when dealing with crypto-assets (par. 2.2.2.4 of the Policy Statement PS-01-2021). CASPs should understand the operating rules, capabilities and limitation of such technologies and verify their integrity on a regular basis. Furthermore, it may be necessary for a CASP to use several complementary tools depending on their business model (Schwarz, 2021).

Although necessary, the use of such tools is not sufficient in itself. Regulated Entities need to understand the risks of crypto-assets in relation to TF across the spectrum of their operations. The level of transaction monitoring should be based on the CASP's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher-risk situations. The adequacy of the CASP's monitoring system and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the CASP's TF risk programme.

Transaction monitoring is an essential component in identifying transactions that do not fit the behaviour expected from a customer's profile or that deviate from the usual pattern of transactions, thus be suspicious. Regulated Entities should monitor transactions for any unusual activity or patterns that may be indicative of TF. This includes monitoring for transactions that are inconsistent with the customer's known business or personal activities, as well as monitoring for transactions involving high-risk countries or individuals. Specifically, Regulated Entities should be aware of common trigger events, such as transactions involving individuals or entities on terrorism watchlists or sanctions lists or adverse media, customer information involving high risk countries, such as IP address in regions known for terrorist activity that may indicate TF activity.

Furthermore, Regulated Entities should consult the following Red Flags Indicators mentioned in FATF Report "Virtual Assets-Red Flag Indicators":

- Technological features that increase anonymity - such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies;
- Geographical risks - criminals can exploit countries with weak, or absent, national measures for virtual assets;
- Transaction patterns - that are irregular, unusual or uncommon which can suggest criminal activity;
- Transaction size and frequency – if the amount and frequency has no logical business explanation;
- Sender or recipient profiles - unusual behaviour can suggest criminal activity;
- Source of funds or wealth - which can relate to criminal activity;

It is important to note that the above list is not exhaustive and that Regulated Entities should use their judgment to identify any suspicious activity.

Detecting and Reporting suspicious transactions

The Regulated Entities should have a full understanding of the customer's economic profile and account activity in order to identify transactions which are suspicious. According to paragraph 9 and Part VI of the CySEC AML/CFT Directive, in cases where a compliance officer decides to notify the Unit for Combating Money Laundering (MOKAS), then he completes a report and submits it to MOKAS as soon as possible.

The Regulated Entities should also implement a system that will allow them to produce the report in a printed form at any time. It is provided that, after the submission of the compliance officer's

report to MOKAS, the accounts involved and any other connected accounts are closely monitored by the compliance officer who, following any directions from MOKAS, thoroughly investigates and examines all the transactions of the accounts.

A list containing examples of what might constitute suspicious transactions/activities related to ML and TF is attached to the Third Appendix of the AML/CFT Directive.

Part B, of the Third Appendix to the CySEC AML/CFT Directive notes legal fund raising methods used by terrorist groups, which among others, include:

- collection of membership dues and/or subscriptions,
- sale of books and other publications,
- cultural and social events,
- donations,
- community solicitations and fund-raising appeals.

This list is not exhaustive nor does it include all types of transactions that may be used, nevertheless it can assist the Regulated Entities and its employees in recognising the main methods used for TF. The detection of any of the transactions contained in the Third Appendix prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

F. EMPLOYEES OBLIGATIONS, EDUCATION AND TRAINING

In view of the paragraph 35 of the CySEC's AML/CFT Directive, the Regulated Entities must ensure that their employees are fully aware of their legal obligations according to the Law and the present Directive by introducing a complete employee's education and training programme.

Regular training is an opportunity for regulated entities to ensure that staff and Board of Directors are aware of the ML/TF risks posed by their activities and the policies, controls and procedures the regulated entity has in place. Staff should be aware of the legal obligations imposed on both them personally and to the regulated entity. Regulated Entities must

comprehend the importance of staff training especially in the identification and reporting of anything that gives grounds for suspicion (CySEC Circular C315).

In order to help detect suspicious activity, Regulated Entities must ensure their staff are appropriately trained and have awareness of trigger events, red flags, TF typologies and what may constitute unusual activity. CASPs should consult both domestic and international guidance to help determine indicators of suspicious activity relevant to their business. Particularly useful sources include the FIU reporting guidelines and NRA, as well as guidance issued by FATF.

In conclusion, Regulated Entities in Cyprus should implement robust AML/CTF measures, including, among others, customer due diligence and transaction monitoring, and should remain vigilant for any red flags that may indicate TF activity. Additionally, Regulated Entities should report to MOKAS any suspicious activity as soon as possible.

All Regulated Entities should consider this Guidance along with the relevant FATF and EBA Guidance, in identifying, assessing and understanding TF risks. As obliged by the regulatory framework, Regulated Entities must implement adequate and appropriate policies, controls and procedures in order to mitigate and manage TF risks effectively.

G. SELECTED SOURCES

Chainalysis, “The 2022 Geography of Cryptocurrency Report”. Available at: https://go.chainalysis.com/geography-of-crypto-2022-report.html

Chainalysis, “The 2023 Crypto Crime Report”, February 2023. Available at: https://go.chainalysis.com/2023-crypto-crime-report.html

Ciphertrace, “Cryptocurrency crime and anti-money laundering”, October 2022. Available at: https://ciphertrace.com/crime-and-anti-money-laundering-report-october-2022/

Cyprus AML Advisory Authority, “Cyprus National Risk Assessment with respect to the introduction of virtual assets in the Republic”, Prepared by Bandman Advisors 2021. Available at: https://mof.gov.cy/assets/modules/wnp/articles/202112/1033/docs/cyprus_nr_virtual_assets_nov2021.pdf

Dion-Schwarz Cynthia & David Manheim & Patrick B. Johnston, “Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats”, RAND Corporation, 2019. Available at: https://www.rand.org/pubs/research_reports/RR3026.html

Elliptic, “The State of Cross-chain Crime 2022”, October, 2022. Available at: https://www.elliptic.co/resources/state-of-cross-chain-crime-report

European Commission, “Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities [SWD(2022) 344 final]”, Brussels, 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554

Europol, “European Union Terrorism Situation and Trend report 2022”. Available at: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

FATF, “Terrorist Financing Risk Assessment Guidance”, July 2019. Available at https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html

FATF, “Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing”, September 2020. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

FATF, “Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers”, October 2021. Available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

Georgiou Jordan, “The Advancement of the Blockchain and Cryptocurrency industry in Cyprus”, 2021. Available at: https://mof.gov.cy/assets/modules/wnp/articles/202111/1016/docs/advancement_blockchain_crypto_cyprus.pdf

Hanley-Giersch Jennifer , “Virtual Currencies-Regulation and Terrorist Financing Risks”, *ACAMS Today*, August 24 2020. Available at: https://www.acamstoday.org/virtual-currencies-regulation-and-terrorist-financing-risks/

Information Exchange Working Group (IEWG), “FIU-FinTech Cooperation and Associated Cybercrime Typologies and Risks”, Egmont Group of Financial Intelligence Units, July 2022. Available at: https://egmontgroup.org/wp-content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc.-Crimes.pdf

Salami Iwa, “Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?”, *Studies in Conflict and Terrorism*, 41 (12), 2017, pp. 968-989. Available at: https://repository.uel.ac.uk/item/84qxv

Schwarz Nadine, Ke Chen, Kristel Poh, Grace Jackson, Kathleen Kao, Francisca Fernando, and Maksym Markevych, “Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism”, *International Monetary Fund*, October 2021. Available at: https://www.imf.org/-/media/Files/Publications/FTN063/2021/English/FTNEA2021003.ashx

Stephen Reimer & Matthew Redhead, “Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks”, RUSI Occasional Paper under project CRAAFT, *Royal United Services Institute for Defence and Security Studies*, April, 2022. Available at: https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/624c339b2bb62359821fa1dd/1649161117463/Bit+By+Bit.pdf

U.S. Department of the Treasury, Office of Public Affairs, “Action Plan to Address Illicit Financing Risks of Digital Assets, September 2022”. Available at: https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf

Whittaker Joe, “The Role of Financial Technologies in US-Based ISIS Terror Plots”, *Studies in Conflict & Terrorism*, September 2022. Available at: https://www.tandfonline.com/doi/full/10.1080/1057610X.2022.2133345?scroll=top&needAccess=true&role=tab