

10/03/2025

**Financial Crime
Compliance**
Tel: (+356) 21441155

To: The Management Body,
To: The Money Laundering Reporting Officer,

Mitigating the Funding of Terrorism and Sanctions Evasion Risks in Crypto-Asset Service Providers and Financial Institutions

You are receiving this letter as the Management Body and/or Money Laundering Reporting Officer of a Crypto-Asset Service Provider or a Financial Institution¹ ("Authorised Entity") supervised by the Malta Financial Services Authority (the "MFSA" or "Authority").

1. BACKGROUND

The rapid growth of the virtual financial services industry globally has spurred significant transformations in the financial sector, with Malta emerging as a key jurisdiction in this evolving landscape. Central to this development are Crypto-Asset Service Providers ("CASPs"), along with Financial Institutions such as E-money Institutions and Payment Service Providers, which collectively form the backbone of the country's digital financial ecosystem. These entities offer critical services, including exchanges, wallet management, digital payments, and custodianship, and are key enablers of Malta's growing position in the crypto-asset/payments industry.

¹ For the purpose of this document, the term "Financial Institutions" refers to authorised entities carrying out licensable activities delineated in the Financial Institutions Act (Cap. 376).

Contemporarily, the Maltese, and overall European financial services sector are faced with two contrasting realities. Firstly, the EU's implementation of its Markets in Crypto-Assets Regulation ("MiCAR") harmonises market rules for an industry that was previously characterised by Member States' vastly diverging supervisory approaches. The MiCAR is anticipated to place crypto services within closer reach of everyday consumers. In parallel, the EU's Instant Payments Regulation and eIDAS Regulation further echo the Union's direction towards an increasingly integrated financial services industry that facilitates access to financial services through technology.

The increasing prominence of crypto-asset services and instant payments is juxtaposed by implications resulting from the geo-political context characterising the EU's periphery and beyond. The implementation of restrictive measures has become a core issue for both those regulating and those being regulated. As such, the financial services industry's expanded diversity can, even unintentionally, result in increased FT risks and heightened exposure to the circumvention of sanctions. As a consequence, stronger mitigating measures may be required.

Malta's 2023 National Risk Assessment ("NRA") comments thoroughly on these risks. For example, Financial Institutions facilitating funds flowing from Malta have been considered from a FT perspective as a result of these Authorised Entities' jurisdictional exposure. Similarly, CASP's geographical reach cannot be understated. As provided by the NRA, cases of suspected FT and connections with terrorist organisations, while limited, have been observed. The likelihood of crypto-assets being abused for sanctions circumvention is also highlighted by the NRA.

In an effort to better understand and assess what are the common, and uncommon, practices with regards to these areas, the Authority conducted a thematic exercise

focusing on the risk assessment and control measures adopted by Financial Institutions and CASPs and meant to mitigate FT/TFS related risks. The exercise was also conducted in anticipation of the increased likelihood of having Financial Institutions applying for MiCAR licences and vice versa. Additionally, this exercise also aligns with the MFSA's, alongside other counterpart authorities', fulfilment of broader national policy goals and objectives established by Malta's National Coordinating Committee on Combating Money Laundering and Funding of Terrorism.

Gathering a high-level overview of the industry's practices also allows the Authority to better communicate its expectations to the industry, which is also the intended purpose of this document.

The expectations provided here complement the implementation of the European Banking Authority's ("EBA") recently published Guidelines on the implementation of *Union and National Restrictive Measures*. It is worth noting that these EBA Guidelines will become applicable as of 30 December 2025. It is also worth bearing in mind that with the eventual application of the EU's AML Package, the overall AML/CFT framework is to be extended to also cover TFS-related aspects. This exercise can therefore be a starting point for CASPs and Financial Institutions to start considering what changes need to be implemented within their overall control frameworks.

2. METHODOLOGY

2.1. Applicability

Bearing in mind the above-mentioned objectives of the thematic exercise it was essential to include the widest possible array of Authorised Entities to ensure that this assessment reached conclusions that are reflective of the overall situation within the industry.

By encompassing operationally active CASPs and Financial Institutions, the exercise ensured comprehensive coverage and provided a complete picture of the industry's practices concerning FT and TFS (i.e., risk assessment, transaction monitoring and sanctions screening).

2.2. The Questionnaire

Considering the population size and the nature of this exercise, a questionnaire circulated via email was circulated to suitable contact points. The questionnaire used for this thematic review comprised a series of both open and closed-ended questions categorised into 5 sections as presented below:

Section 1	Risk Understanding	This section was solely dedicated to inquiring how CASPs and Financial Institutions consider risks related to FT/TFS within their general risk assessment/management framework. Questions were directly related to the conduct of Business Risk Assessments and Authorised Entities' risk
------------------	--------------------	---

		appetites. Specific questions also related directly to both Jurisdiction and Customer Risk Assessments.
Section 2	Controls	This section presented questions related to how Authorised Entities' senior management are kept informed on FT/TFS related matters, mitigating measures related to FT/TFS, and potential considerations being given to the implementation of new technologies.
Section 3	Client Screening	This section presented an array of questions related to Authorised Entities' client screening practices, namely whether CASPs and Financial Institutions utilise an automated system, screening frequency, their system's flexibility, and testing.
Section 4	Transaction Monitoring	This section presented an array of questions related to Authorised Entities' transaction monitoring practices, namely whether CASPs and Financial Institutions utilise an automated system, frequency, red flags/alerts, and monitoring rules/parameters.
Section 5	Training and Awareness	This section inquired on Authorised Entities' training initiatives related to FT/TFS.

3. KEY FINDINGS

This section is dedicated towards providing a descriptive rendition of the trends and practices resulting from the industry's responses. Percentages provided have been rounded to the nearest value. This section also explains the Authority's supervisory expectations according to the relevant themes.

3.1. Risk Understanding

49% of respondents stated that according to their understanding their sector's residual risk exposure is 'medium'. Furthermore, when inquired to indicate the level of entity-specific risk exposure to FT 54% of Authorised Entities indicated a low level of risk exposure. While most respondents (92%) stated that they have considered the 2023 NRA results within their BRA, 8% stated that they did not.

The majority of respondents indicated that they re-assess their FT risk exposure in the BRA every year, with the exception of 2 respondents who indicated that they do so every 2 years. When asked if there are any industries, customer types, or geographies, which they have deemed to fall outside of their risk appetite for FT/TFS, the majority replied that they do, with only 16% indicating that they do not. Among those who answered in the affirmative, the most commonly cited areas of concern were customers who had links to either sanctioned jurisdictions or jurisdictions that are heavily exposed to sectoral sanctions, opaque ownership structures, high-risk jurisdictions and industries relating to the adult entertainment and defence industries.

With respect to the Jurisdictional Risk Assessment ("JRA"), 96% of respondents indicated that they conduct an independent JRA. All respondents indicated that they

consider FT risks in the JRA, while 84% and 96% of respondents indicated that they consider Proliferation Financing and TFS risks, respectively. When inquired to list the major three external sources which they use for the compilation of the JRA, the most common replies were FATF Lists, EU Sanctions list and the Basel AML Index. All respondents indicated that the most recent review was carried out in the last calendar year and when asked for the reason behind the latest revision, the majority (72%) indicated that this was a 'procedural review'.

Respondents listed suspicious and complex transactions, adverse media and material changes in the customer profile, as the most prevalent trigger events that may lead to the re-evaluation of the customer's risk score. Other non-prevalent trigger events that were mentioned included suspicious customer behaviour, regulatory and/or enforcement action on customers and changes in the frequency of cash withdrawals. From the services offered, the majority of respondents indicated that they consider Payment Services and the Issuance of Electronic Money as the most prone to be exploited for FT.

To assess the sector's appetite towards adopting new technologies, respondents were asked whether they believe emerging risks from such implementations could heighten exposure to FT. The majority (64%) indicated they do not believe these risks would increase their FT exposure. Among those who mentioned that new technologies may increase their risk exposure, the majority identified the potential exploitation of the Entity's systems by terrorists and the failure of AI-operated transaction monitoring systems as the key concerns.

3.1.1. Supervisory Expectations

Authorised Entities are reminded that the PMLFTR obliges the consideration of the EU's Supranational Risk Assessment (SNRA) as well as any National Risk Assessments. Thus, those Entities who have yet to consider Malta's NRA in their BRA are to refer to Regulation 5(1) of the PMLFTR and Section 3.3 of the FIAU's Implementing Procedures.

The PMLFTR imposes an obligation on Authorised Entities to take appropriate steps, proportionate to the nature and size of their business, to identify and assess the risks of ML/FT that arise out of its activities or business. When it comes to the updating of the BRA, Authorised Entities are to refer to Regulation 5 of the PMLFTR and to Section 3.3.4. of the Implementing Procedures – Part I. Furthermore, Authorised Entities should consider whether there have been any changes that may require a review and, if necessary, an update of its BRA.

As part of the measures, policies, controls, and procedures that an Authorised Entity is to implement, it is especially important that it adopts and applies a Customer Acceptance Policy. This policy should clearly outline the types of customers likely to pose a higher-than-average risk of ML and FT and specify the circumstances under which the Entity will decline to service someone. While the Authority recognises that an Authorised Entity may make exceptions to its CAP, it is essential that the reasoning for doing so is duly documented, there are adequate mitigating measures put in place and that the situation is properly monitored to ensure that it is at all times aware of the risks it is facing. What would be especially important, absent a review of the CAP itself, is that the exception does not become the rule.

With respect to the drafting of a JRA, while it is not necessary that Authorised Entities carry out an independent JRA themselves, any adoption of third-party JRA is to be done following due consideration that it reflects the particular circumstances of the Authorised Entity, including its business activities, and to ensure that any assessment and associated risk rating is updated periodically. Authorised Entities are to refer to Section 8.1 of the FIAU's Implementing Procedures where a number of sources to be consulted are listed to identify non-reputable and/or high-risk jurisdictions. Key sources, among others, include, (i) FATF Public Documents (ii) Commission Delegated Regulation (EU) 2016/1675 Identifying high-risk third countries with strategic deficiencies and (iii) Statements and/or Declarations issued by the FATF or by an FATF-Style Regional Body which also reflect FT concerns. Those Entities who are not currently considering these sources are to bear in mind that this could potentially lead to regulatory action by the relevant authority should this situation persist.

The Authority's expectations are not only driven by what is stipulated locally but also at European level. The EBA's Guidelines on the implementation of Union and national restrictive measures provide ample information in this regard. From a risk assessment/understanding perspective, the EBA provides its guidance on conducting a 'restrictive measures exposure assessment'. This assessment should provide Authorised Entities with a better understanding as to which area of their business is exposed to restrictive measures or vulnerable to sanctions circumvention. This document is not intended to reiterate what the EBA's Guidelines already provide. While the said Guidelines are not strictly applicable, Authorised Entities are highly encouraged to refer to these set of Guidelines in more detail.

3.2. Controls

While the majority of respondents (94%) indicated that they consider the entity's risk exposure to FT in their MLRO report, a small number of respondents indicated that they do not. Among those who indicated that they consider FT, the most common replies were that they consider transaction risk exposure (82%) and business risk exposure (80%).

Lastly the questionnaire further inquired on whether the given Authorised Entity is utilising new technologies² in their internal control framework to more effectively address risks related to FT/TFS. In this respect, 10% of CASPs indicated that they do not implement new technologies in their control framework. 73% of E-Money Institutions and Payment Institutions also noted that they do not implement any forms of new technologies as part of the mitigating measures. With respect to whether they have any future plans to further expand into the use of Artificial Intelligence, Machine Learning and Blockchain Analysis within their control framework, 52% of all respondents indicated that they are interested, whilst 48% indicated that they do not have any future plans on the use of new technologies.

3.2.1. *Supervisory Expectations*

Regulation 5(5) of the PMLFTR provides that an Authorised Entity must have in place measures, policies, controls and procedures to address any identified risks. Furthermore, the PMLFTR places considerable emphasis on the need to conduct

² For the purpose of this document, the term "new technologies" refers to innovative tools, systems, and methods that leverage advancements in fields like data analytics, artificial intelligence (AI), machine learning, blockchain, cloud computing, biometrics, and digital identity solutions designed to enhance the efficiency, accuracy, and effectiveness of processes aimed at detecting, preventing, and mitigating ML/FT risks.

ongoing monitoring on the Entity's customer base. This is further elaborated on by the FIAU's Implementing Procedures, which state that once an Authorised Entity has identified the ML/FT risks it is exposed to, measures must be adopted to prevent these risks from materialising or at least mitigate their occurrence as much as possible on an ongoing basis.

Given the increasing reliance on digital platforms for financial transactions, the sheer volume and speed at which transactions are now processed may necessitate the adoption of advanced technological solutions to enhance risk management. Artificial intelligence and machine learning can play a crucial role in identifying suspicious transaction patterns in real-time, enabling institutions to detect and prevent potential FT and TFS evasion more effectively. Big Data analytics can further enhance Authorised Entities' risk-based approach by providing deeper insights into customer behaviour and transactional anomalies.

Moreover, with the rise of crypto-assets, Financial Institutions must consider the unique risks posed by un-hosted wallets, which may facilitate anonymous transactions and obscure beneficial ownership. However, blockchain analytics tools can help mitigate these risks by enabling enhanced transaction tracing, identifying wallet clusters linked to high-risk entities, and monitoring for illicit activity. Regulatory technology ("RegTech") solutions can further support compliance efforts by automating sanctions screening, customer due diligence, and transaction monitoring, ensuring that Financial Institutions remain aligned with regulatory requirements in a fast-evolving digital landscape.

By leveraging these technological advancements, Authorised Entities can strengthen their financial crime risk management frameworks, improve the efficiency of

compliance processes, and enhance their ability to detect and prevent illicit financial flows.

3.3. Client Name Screening

A large majority of respondents (92%) indicated that their sanctions screening system is third-party provided³. Nevertheless, 10% claimed that their screening practices are conducted manually. Considering this, 53% indicated that the frequency of their customer screening occurs in real-time⁴ and 41% as daily. 6% indicated that their clients are screened on a weekly/bi-weekly (once every two weeks) basis. Out of all respondents, 6% indicated that their implemented systems do not facilitate the timely detection of clients/involved parties having control/ownership of legal entities immediately after changes are implemented within the considered sanctions lists.

While 56% reported that they review their systems (e.g., recalibration of systems after considering false positives or rechecking applicability of considered lists) either annually or semi-annually (once every 6 months), 12% indicated that their systems are reviewed less than once every year. One fifth (20%) of the respondents also provided that their screening practices do not include the beneficiaries/merchants (counterparties) that their clients transact with. Furthermore, 4% provided that they do not consider the ownership and control structure of their clients which are legal entities.

³ For the purpose of this document, the term 'third-party provided' refers to instances where Authorised Entities make use of third-party solutions which they operate themselves.

⁴ In this context, 'real-time' means that screening is constantly conducted at every passing moment. Therefore, implying that any changes to sanctions lists are immediately considered by the given Authorised Entities.

12% of respondents provided that they do not consider other lists apart from domestic, EU, and UN lists. Of those that do consider lists other than those mentioned, 40 respondents indicated that they consider OFAC, while 29 provided that they also screen their clients against OFSI lists.

3.3.1. Supervisory Expectations

While the Authority understands that Authorised Entities may implement tools provided by third parties, the ultimate responsibility for compliance with TFS and restrictive measures still lies with that particular entity. The Authority also identifies that Authorised Entities' needs with regards to sanctions screening may differ from one another especially when considering modest client bases. Authorised Entities are encouraged to carry out sanctions risk exposure assessments to ascertain whether they need to explore different screening methodologies or whether their current practices are in line with what their current circumstances offer. This same concept applies to ensuring whether the frequency of name screening is commensurate with the client base being upheld.

While Authorised Entities may be categorised by their type of licence, each individual entity differs from another by its specific business model. Hence, the applicability of screening different types of client information differs from one entity to another. As such, Authorised Entities' policies and procedures should delineate the types of data/information the entity intends to screen. Commensurate to this, Authorised Entities should assess the accuracy of the client information they hold to facilitate their determinations on whether a beneficiary, any person, body, legal person or entity is subject to restrictive measures. An approach of this kind will ensure a consistent methodology towards screening across different types of clients within

the same client population. Moreover, Authorised Entities' policies and procedures should outline the applicable EU and UN lists against which its client population should be screened. Authorised Entities may consider delineating other lists of any third-country sanctions in accordance with their risk-appetite.

Complimentary to the above, Authorised Entities are reminded to refer to the Sanctions Monitoring Board's Guidance Note on the Application of Article 17(6)(a) (b) and (c) of the National Interest Enabling Powers Act.

3.4. Transaction Monitoring

14% of respondents provided that their transaction monitoring is based on a manual procedure, while 68% provided that they utilise a combination of both manual checks and automated systems. A separate 18% submitted that their transaction monitoring procedures are solely based on the implementation of an automated system. The majority of respondents (60%) indicated that the automated systems they utilise are third-party provided.

Of those Authorised Entities that utilise an automated system, 33% provided that their algorithms do not provide specific functionality which considers earlier false positives. Moreover, 20% of respondents indicated that their automated solutions do not host specific features that facilitate the detection of suspicious activity related to funding of terrorism, proliferation financing, and sanctions circumvention. Additionally, 36% of the population of Authorised Entities in scope of this thematic exercise noted that the automated systems that they utilise are unable to automatically detect significant changes both in volume and value of client transactions. 32% further indicated that their automated solutions are unable to detect transactions being carried out in rapid succession. Furthermore, only 12% of

the respondent Authorised Entities provided that their transaction monitoring practices include rules specific for funding of terrorism.

3.4.1. Supervisory Expectations

Authorised Entities are expected to have a transaction monitoring system of a level of complexity that is commensurate to the given Entity's business model, products, and customer population. Said system should be able to facilitate the identification of unusual behaviour or transactions that diverge from usual customer activity. While automated systems may not always be called for, it becomes more difficult not to implement elements of automation when the volume of transactions being processed is considerable and especially the speed with which transactions are to be processed.

Authorised entities should implement a risk-based approach to transaction monitoring and increase the level of scrutiny when high-risk transactions are identified. In these scenarios Authorised Entities might be required to identify additional elements of the transaction including the source of funds, any new operational activities, any significant relevant changes relating to the given customer, and any other information that the Authorised Entity deems reasonably necessary to be satisfied that the funds are derived from a legitimate source.

There is copious material available setting out how the obligation of transaction monitoring and scrutiny is to be effectively abided by. Authorised Entities are reminded to refer to the Implementing Procedures – Part I, the Guidance Note: A Look Through the Obligation of Transaction Monitoring and a dedicated Questions and Answers Document on Transaction Monitoring.



CASPs should in particular be careful not to be over-reliant on blockchain analytical tools when it comes to transaction monitoring. These tools complement more traditional forms of transaction monitoring carried out through risk-based transaction monitoring programs in line with the requirements of Regulation 7(2) and Regulation 11(9) of the PMLFTR, as well as Section 4.5 of the FIAU's Implementing Procedures - Part I and the relevant sections of the Implementing Procedures - Part II addressed to CASPs. Any such program should include systems to monitor transactions based on assessed risk levels and depending on the type of crypto-asset service and technology used. The program should incorporate processes to identify ML/FT typologies, such as large fiat deposits followed by fund transfers without acquiring crypto-assets or the use of tumblers and mixers, and should establish and compare customer transaction profiles, flagging inconsistencies or sudden changes. The program must also identify patterns like the use of multiple wallets or wallet changes for the same crypto-asset and link accounts controlled by the same customer. This comprehensive approach enables CASPs to adapt to evolving risks and maintain a robust CFT framework.

3.5. Training and Awareness

Respondents indicated that the consideration of FT/TFS within their training efforts is a common practice, with 98% of respondents providing such training to their staff. Additionally, 88% conduct this training at least once a year, suggesting a routine approach to maintaining awareness and promoting a compliance culture.

3.5.1. Supervisory Expectations

The MFSA recognises that informed staff can enhance the effectiveness of the MLRO within an Authorised Entity. The MFSA continues to encourage MLROs and other CFT compliance professionals to ensure that staff receive tailored training specifically related to FT in line with their roles and responsibilities. Where applicable, MLROs are also encouraged to provide training themselves and to oversee the delivery and quality of such training. The active involvement of MLROs in training initiatives can enhance Authorised Entities' overall CFT compliance frameworks by ensuring that employees clearly understand relevant FT related risks, are able to identify what should be reported, and reduce false positives. Given that as a matter of practice, these same officers are usually also entrusted with sanction-related functions, the above is also applicable with regards to TFS.

4. CONCLUSION

The findings from this review are being shared in this letter to highlight key observations, draw attention to common practices, and identify areas requiring further improvement within the sector. The aim is to reinforce governance and enhance the compliance culture among CASPs and Financial Institutions.

The observations provided here are commensurate to a reality where aspects of CFT/TFS within Financial Institutions and CASPs still require further improvement. As such, the supervisory expectations being communicated by this content presents several opportunities for Financial Institutions and CASPs to consider and ultimately improve their CFT/TFS frameworks. In sum, Financial Institutions and CASPs should:

- Continue providing relevant training to enhance their staff's understanding of FT/TFS-related risks and regulatory obligations,
- Ensure that they consider the latest iteration of Malta's NRA in their risk assessments,
- Take steps and consider conducting a sanctions risk exposure assessment in anticipation of forthcoming obligations in this regard,
- Ensure that systems/solutions implemented via third party providers are not overly depended upon and that reviews of such systems are independently carried out. Authorised Entities should ensure that these systems/solutions are adequate,
- Ensure that their policies and procedures specifically delineate applicable sanctions lists , and
- Potentially consider the implementation of new technologies to ensure that the complexity of their controls is commensurate to the services they offer.

The MFSA encourages Authorised Entities and MLROs to review this document alongside other relevant guidance, such as the MFSA's Guidance for MLROs in the Financial Services Sector and the Financial Intelligence Analysis Unit's issued guidance. The findings outlined in this report may inform the Authority's future outcomes-based supervision in the area of financial crime compliance. Authorised entities should use this report as an opportunity to assess and strengthen their CFT and sanctions frameworks, ensuring they meet regulatory expectations.

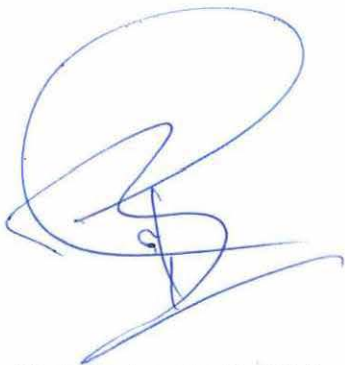
The MFSA extends its appreciation to all CASPs and Financial Institutions that participated in this exercise for their cooperation. Should any aspects remain unclear or further clarification on meeting the Authority's expectations be needed, Authorised Entities are encouraged to reach out to the Authority and Sanctions Monitoring Board for any sanctions related issues. The MFSA remains committed to

ms

providing ongoing guidance to support best practices and enhance governance and compliance standards in the virtual financial services industry.

Yours Sincerely,

Malta Financial Services Authority



Dr Christopher P. Buttigieg
Chief Officer Supervision



Matthew Scicluna
Head
Financial Crime Compliance

The MFSA ensures that any processing of personal data is conducted in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation), the Data Protection Act (Chapter 586 of the Laws of Malta) and any other relevant European Union and national law. For further details, you may refer to the MFSA Privacy Notice available on the MFSA webpage www.mfsa.mt.