17th June 2026

Financial Crime Compliance

Tel: (+356) 21441155

To: The Management Body,

To: The Money Laundering Reporting Officer,

Mitigating Terrorist Financing, Proliferation Financing and Targeted Financial Sanctions Evasion Risks in Credit Institutions

You are receiving this letter as the Management Body and/or Money Laundering Reporting Officer of a Maltese licensed Credit Institution ("Authorised Entity") supervised by the Malta Financial Services Authority (the "MFSA" or "Authority").

1. BACKGROUND

Terrorist financing ("TF"), proliferation financing ("PF"), and targeted financial sanctions ("TFS") evasion continue to represent significant and evolving threats to the stability and integrity of the global financial system. The FATF's Comprehensive Update on Terrorist Financing Risks highlights that, while the overall reliance on traditional financial services by terrorist groups has decreased, these channels remain actively exploited to facilitate fundraising, movement, and access to funds.

At the same time, the FATF observes a growing convergence between traditional financing channels - such as the use of cash and hawala and other similar service

providers- and emerging digital technologies, adding new layers of complexity to TF activities. Similarly, the FATF's report on Complex Proliferation Financing and Sanctions Evasion Schemes, underscores the sophistication with which illicit actors seek to evade sanctions and circumvent controls aimed at preventing PF.

These developments, taken together with Malta's national risk profile, underline the critical necessity for Credit Institutions to **maintain robust, adaptive, and forward-looking control frameworks**. Authorised Entities must be capable of identifying, assessing, and mitigating TF, PF, and TFS evasion risks within an environment characterised by increasingly sophisticated typologies and rapidly developing technologies. Strengthening effectiveness in mitigating these areas is essential to **safeguard Malta's financial system** and contribute to the broader international effort to combat illicit finance.

2. METHODOLOGY

2.1. Applicability

The selection of Credit Institutions and the areas of focus for this thematic exercise, being TF, PF and TFS evasion were informed by Malta's latest iteration of the National Risk Assessment ("NRA") and by recent international regulatory developments, including the EU Instant Payments Regulation, the EBA's Restrictive Measures Guidelines (EBA/GL/2024/14) and recent FATF publications.

Malta's NRA identifies the banking sector as being among the most exposed sectors to TF, PF and to TFS evasion, owing to its central role in the movement of funds. The

NRA also notes that the **effectiveness of institutions' reporting of suspicious transaction reports**, **conducting of customer due diligence**, **risk assessment frameworks**, **transaction monitoring**, and **sanctions screening control** remain a key determinant of their capacity to mitigate these risks.

This exercise forms part of broader national effort and builds on a previous iteration which assessed industry practices among Financial Institutions and Crypto-Asset Service Providers in relation to mitigating the financing of terrorism and sanctions evasion.

2.2. Sample Selection

To ensure a robust, risk-sensitive and holistic view, this thematic review places **all MFSA-licensed Credit Institutions** in scope of the exercise. The population includes both locally-incorporated banks and branches of foreign banks established and operating in Malta. By encompassing all active Credit Institutions, the exercise provides comprehensive coverage and a complete, comparable view of industry practices in countering the financing of terrorism ("CFT"), counter proliferation financing ("CPF") and TFS.

2.3. The Questionnaire

Given the breadth of the in-scope population and the comparative nature of this review, an electronic questionnaire distributed *via* direct email was selected as the most appropriate tool. The questionnaire comprised a series of closed-ended and open-ended questions and was categorised into **six sections** as described below:

Section 1	**Risk Understanding and Governance**	This section assesses how effectively Authorised Entities understand and govern their TF, PF and exposure to TFS evasion risk, including the quality of their restrictive-measures exposure assessments, formal TF and PF risk assessments, jurisdictional risk assessment, customer risk assessments, business risk assessments, Board reporting, and their consideration of risks arising from the Instant Payments Regulation.
Section 2	**Identification and Verification**	This section explores the adequacy of customer identification controls, focusing specifically on the use of automated tools to detect forged or falsified identity documents.
Section 3	**Transaction Monitoring**	This section evaluates whether Authorised Entities maintain appropriate transaction-monitoring systems, how well CFT and TFS' typologies are embedded, the strength of rules and detection capabilities, and the extent to which specific products and services receive tailored monitoring. The section also assesses the changes adopted to their systems in view of the Instant Payments Regulation.
Section 4	**Sanctions Screening**	This section reviews the robustness of sanctions screening frameworks, including systems used, lists applied/consulted, screening frequency, testing and updating arrangements, and the effectiveness of asset-freezing procedures. The section also assesses the changes adopted to sanctions screening practices in view of the Instant Payments Regulation.

Section 5	**Artificial Intelligence**	This section examines the current and planned use of artificial intelligence ("AI"), including the types of AI tools being adopted, their features, and financial-crime-related use cases.
Section 6	**Training and Awareness**	This section examines the adequacy of CFT, CPF and TFS' training programmes, focusing on role-appropriate and ongoing training.

3. KEY FINDINGS

This section provides a descriptive and anonymised rendition of the trends and practices evidenced in the responses provided, organised by the thematic areas of focus as set out in Section 2.3. In parallel, each section also highlights any identified good practices, benchmarked against the Authority's supervisory expectations. Percentages presented, are rounded to the nearest value.

3.1. Risk Understanding and Governance

When asked to rate the sector's inherent TF risk, a majority assessed exposure at the higher end of the spectrum, with 57% of respondents replying to Medium-High and a further 33% replying Medium. This broadly aligns with the NRA which classifies the movement of funds for TF via Credit Institutions as posing a Medium residual risk. Consistent with this alignment, 62% of respondents reported using the NRA to inform TF elements of their business risk assessment, while 57% did so for PF. Several

institutions also indicated that the NRA is used as a primary input to their jurisdictional risk assessments. Replies provided with respect to risk awareness on restrictive measures[1], reflect a solid momentum on sanctions governance. Across the population, 67% of entities, report having conducted a restrictive-measures exposure assessment while 81% indicate that the management body and/or senior management receive regular TFS reporting. In addition, 90% have formally appointed a senior staff member with responsibility for ensuring compliance with restrictive measures. When asked to reflect on whether the introduction of instant payments, increased the potential TF risks, the majority replied in the affirmative, though several noted that appropriate mitigating measures are being applied to manage this risk effectively.

Relative to TF and TFS evasion, PF controls are not being prioritised across all Authorised Entities. This observation is corroborated in several replies provided. While all respondents maintain a formal risk assessment that consider TF, only 71% maintain a risk assessment that considers PF. Additionally, whilst 81% of respondents reported regular updating to the board and/or senior management on risk factors related to TF, this falls to 62% in the case of PF risk factors. Policy coverage shows a similar trend. CFT specific policies are in place at 100% of institutions and TFS specific policies at 90%, yet only 67% maintain dedicated CPF policies and procedures.

Supervisory Expectations

It is very positive that many Credit Institutions are **aligning their entity-level assessments with Malta's NRA** and making substantive use of it in their

[1] *European Union or domestic restrictive measures or restrictive measures resulting from a United Nations Security Council Resolution*

frameworks. At the same time, the Authority reminds all Authorised Entities that Regulation 5(1) of the PMLFTR requires subject persons to identify and assess money laundering ("ML") and TF risks and **to take into consideration both national and supranational risk assessments** when conducting their business risk assessment. Non-integration of the NRA therefore constitutes a regulatory gap that must be remedied without delay. The Authority expects entities to **keep this linkage current** by periodically refreshing NRA-derived assumptions.

Most Authorised Entities have reported close alignment with the **EBA's Restrictive Measures Guidelines** (EBA/GL/2024/14) and the recently revised National Interest (Enabling Powers) Act, 2025. Authorised Entities are expected to take appropriate steps, proportionate to the nature and size of their business, to **identify and assess the risks of violations of restrictive measures and proliferation financing and circumvention** thereof that arise out of its activities or business. These steps shall take into account risk factors, including those relating to clients, geographical areas, products, services, transactions and delivery channels. Authorised Entities are to ensure that the risk assessment is regularly reviewed and kept up to date.

In line with the EBA/GL/2024/14**,** the management body should be informed of the latest restrictive measures exposure assessment. They should also oversee and monitor, through internal controls function, the extent to which the restrictive measures policies and procedures are adequate and effective. Management body should **assess the effectiveness** of the restrictive measures' compliance function at least annually. In parallel, the EBA/GL/2024/14 expects that Authorised Entities **appoint a senior staff member** in charge of compliance with restrictive measures. The designated staff member is expected to have the knowledge and understanding of restrictive measures to fulfil their function effectively.

It was also very positive to note that many Authorised Entities **appropriately considered the jurisdictional element** when identifying customer typologies related to TF and PF risks. In line with the FIAU's Implementing Procedures, Authorised Entities are required to assess the jurisdictional risk in determining the level of ML and TF risk presented. In meeting this obligation, Entities are expected to go beyond simply identifying non-reputable jurisdictions and to assess the specific risk factors associated with each jurisdiction. Entities are to ensure that any such assessment and associated risk rating is **updated periodically**.

3.2. Identification and Verification

Implementation of dedicated systems to detect forged and fake identification documents, is broadly consistent with the fact that the majority of Credit Institutions in Malta onboard customers through face-to-face interactions. In fact, among respondents reporting the adoption of such systems (24%), these tools are predominantly used for digital onboarding (80%), with the most common functionalities relating to document scanning/optical verification (80%) and, to a lesser extent, biometric verification (60%).

When queried on the detection rates of such tools, only 20% of respondents indicated that their systems had successfully detected forged or fake documents in the past 12 months. Follow-up action in such instances included the rejection of onboarding application and subsequent reporting. Control assurance is similarly limited, with only 40% confirming at least annual independent testing.

Supervisory Expectations

In line with Regulation 7(1)(a) of the PMLFTR, Authorised Entities must conduct customer **identification and verification using reliable and independent sources** and apply measures on a risk-sensitive basis, including but not limited to secure remote/electronic means (such as notified e-IDs under eIDAS), where appropriate. This expectation applies regardless, whether identities are verified digitally or manually. As part of their ongoing monitoring obligations, in line with Regulation 7(2)(b) of the PMLFTR, Authorised Entities must ensure that the documents, date or information held are regularly reviewed and kept up to date.

When considering the procurement and deployment of identity-verification systems and tools, Authorised Entities should ensure that the **solution's capability and assurance level are appropriate** for their intended use and be satisfied that the authentication checks are sufficiently reliable to detect forged or fake documents. While digital ID verification systems provide security features that mitigate some issues with paper-based systems, they also increase some risks, such as data loss, data corruption or misuse of data due to unauthorised access. Thus, when selecting electronic identity verification systems, Authorised Entities **must consider data-protection requirements** and satisfy themselves that providers comply with applicable obligations under the EU data-protection framework.

Authorised Entities using such tools must keep electronic copies of identification documents and onboarding images. Such records should be automatically stored through the same system, with the date and time of receipt fully recorded. In addition, the system should have measures in place to ensure that these records cannot be altered or tampered with, in line with the FIAU Implementing Procedures. In instances where the tool is used for customer onboarding, in line with the EBA's Guidelines on Remote Customer Onboarding, Authorised Entities should consider the

most effective way to monitor the ongoing adequacy and reliability of the remote customer onboarding solutions including quality assurance testing and sample testing.

3.3. Transaction Monitoring

Transaction monitoring controls are in place, with variations in the controls **reflecting the differing sizes, complexities, and business models** of Maltese-licensed Credit Institutions. The absolute majority of Authorised Entities indicated that that they screen payment messages prior to settlement. Among those entities which use an automated transaction monitoring system, the majority (75%) replied that algorithms are calibrated to account for false positives.

Scenario coverage embedded within the transaction monitoring systems is broadly focused on the core TF, PF and TFS typologies. Two common typologies identified across all the three assessed risks were the involvement of high-risk jurisdictions and transactions which are not consistent with the customer's risk profile. Other typologies mentioned included the rapid movement of funds for TF, the use of dual-use goods for PF and large value transactions for sanctions evasion. From a rules-and-analytics perspective, 75% of respondents indicated that their transaction monitoring tool can detect significant changes in transaction volume at client level, 81% can detect significant changes in value, and 87% can flag multiple transactions executed in rapid succession by the same client.

When asked how trade finance activities are overseen, respondents commonly cited the use of real-time payment screening to flag restricted items, including those captured under EU dual-use regulations, supplemented by manual reviews and

checks to ensure that goods descriptions accurately align with dual-use control lists. Meanwhile, when asked how personal accounts are monitored for PF, respondents highlighted the use of real-time screening against restricted-items lists, supported by both pre-transaction and post-transaction monitoring to detect any activity indicative of proliferation-related risk.

When asked how transaction monitoring has been adapted as a result of the EU Instant Payments Regulation, many cited that they have introduced additional post-transaction monitoring checks to accommodate the real-time nature of instant payments, whereas a smaller group reported that no changes had been made to their existing systems. Others highlighted the implementation of instant-payment-specific monitoring scenarios, and updates which enable their systems to distinguish between instant and regular payment flows. Implementation of the Regulation's specialised payee-verification requirements was also generally positive, with most Credit Institutions indicating that their processes had been aligned to the new standards.

Supervisory Expectations

Once a business relationship is formed, Regulation 7(2)(a) of the PMLFTR requires Authorised Entities to carry out **ongoing monitoring including the scrutiny of transactions** through transaction monitoring. To ensure compliance with EU asset-freezing and sanctions regulations, Authorised Entities are required to implement controls that identify transactions involving designated persons, entities or jurisdictions. in line with Article 32 of the revised National Interest (Enabling Powers) Act, 2025.

In line with Regulation 11(9) of the PMLFTR, Authorised Entities shall carry out sufficient monitoring of transactions and business relationships to **enable the detection of unusual or suspicious transactions**, including a significant change in the value, volume and frequency of transactions and the carrying out of a number of transactions in rapid succession. It is therefore positive to note that the majority of respondents indicated that their transaction monitoring tool is capable of detecting such activity.

Authorised Entities are expected to determine, on a **proportionate and risk-sensitive basis**, whether transaction monitoring is to be performed manually, through an automated tool, or via a hybrid approach. Such determination should be informed by the Authorised Entity's size, customer base, transaction volumes and value and inherent risks, in line with the FIAU's Implementing Procedures.

Where an automated solution is deployed, Authorised Entities must evidence **governance and transparency over the scenarios, typologies and detection** rules in use, how these are compatible with the products and services offered, and how parameters can be tailored to customer segments and adapted when the relationship changes, consistent with the EBA ML/TF Risk Factors Guidance and any other applicable regulatory or supervisory guidance. Systems should maintain audit trails of alerts and subsequent decisions taken.

Detection rules must be relevant and proportionate to the specific product or service and to the customer's business and risk profile. Authorised Entities should not rely solely on automated rules but must complement such thresholds with documented expert judgement to identify behaviours, patterns, and risks that may not be fully captured through rule-based detection. Transaction monitoring rules should be **periodically tested and fine-tuned** to ensure true suspicious activity is

detected while minimising false positives, with results feeding back into model thresholds and segmentation. **Rule libraries must be kept current with evolving typologies**, particularly for TF, PF and sanctions evasion risks respectively, drawing on indicators and red flags as set out in the EBA's Fifth Opinion on ML/TF risks and FATF issued Guidance, and updated whenever risk assessments, products or channels change.

Authorised Entities are reminded that the EU Instant Payments Regulation mandates an **immediate verification of payee process**, i.e. the payee's name must be checked as soon as the payer enters the payment details and before the payer is allowed to authorise the transaction. Authorised Entities are encouraged to consult the FIAU and Central Bank of Malta joint Q&A Document, which provides further guidance on the application of AML/CFT obligations in the context of instant payments.

3.4. Sanctions Screening

Across the population, sanctions screening is automated and predominantly third-party enabled. A majority (67%) rely on external providers for sanctions screening, while only 5% operate fully in-house solutions. Coverage of sanctions lists appear broadly aligned to recognised sources. For TF, Entities commonly cited the EU (90%), OFAC (86%), and UNSC (86%) lists. Meanwhile for PF, the pattern is similar, with UNSC (86%), EU (81%), and OFAC (76%) lists are most frequently referenced. All respondents replied that their screening tools are either updated real time or within 24-48 hours of an update in the lists screened against.

The majority of respondents who have reported full implementation of the EU Instant Payments Regulation, confirmed that their sanctions-screening mechanisms have

been adapted to ensure daily screening of all customers, as required under the framework. A number of respondents further indicated that they conduct customer screening multiple times per day, thereby demonstrating practices that exceed the minimum regulatory requirements. When asked whether respondents have experienced instances where assets needed to be frozen, 33% replied in the affirmative. Among these, the majority report implementation within 24 hours, indicating an ability to operationalise restrictive-measures requirements at pace. Control assurance reflects varying levels of maturity. While 38% of respondents report conducting periodic testing of their screening systems on a quarterly basis, and another 38% on an annual basis, others indicated that they perform such testing even less frequently.

Supervisory Expectations

Given the sector's reliance on automated, largely third-party–enabled screening systems, Authorised Entities are expected to **evidence robust outsourcing governance**. When outsourcing arrangements are in place, Authorised Entities shall carry out a regular control of compliance by the service provider, **assess the effectiveness** of the services covered by the agreement and take any needed mitigating measures. These expectations flow from the FIAU Implementing Procedures and EBA's Restrictive Measures Guidelines (EBA/GL/2024/14). Where screening is performed by a vendor, the Authorised Entity **retains full responsibility for compliance** and must be able to demonstrate that the tool ingests EU and UN lists without delay.

In parallel, Authorised Entities offering instant euro credit transfers must meet the requirements emanating from the revised National Interest (Enabling Powers) Act and the transposed EU Instant Payments Regulation's requirement to verify, at least

daily, that their **users are not subject to EU targeted financial restrictive measures**. Authorised Entities are not required to apply transaction-based screening for instant credit transfers, however, they are to carry out **daily screening** of all customers, as well as immediate re-screening **whenever new EU targeted financial restrictive measures or amendments enter into force**.

Screening coverage must **align first and foremost with binding local, EU and UN regimes.** In line with SMB Guidance, OFAC and other lists shall be used as risk-based supplements where appropriate. Specifically, FATF Recommendation 6 requires each country to implement the TFS regimes to comply with the United Nations Security Council Resolutions relating to the prevention and suppression of terrorism/ terrorist financing (i.e. UNSCR 1267 (1999) and UNSCR 1373 (2001)). Meanwhile, FATF Recommendation 7 requires each country to implement TFS relating to the prevention of weapons of mass destruction proliferation which are contained in the relevant UNSCRs. Authorised Entities are expected to have in place policies and procedures to suspend, **without delay**[2], operations triggering an alert of a possible match with a designated person or entity, or owned, held or controlled by a designated person or entity, or whose beneficial owner is a designated person.

In line with EBA's Restrictive Measures Guidelines (EBA/GL/2024/14), Authorised Entities should **regularly test their screening system** settings to determine whether the screening system remains appropriate in light of Authorised Entities' restrictive measures exposure assessment, and that it remains effective. Authorised Entities should determine the **frequency and intensity of checks** based on the restrictive measures exposure assessment and record them in their policies and procedures. Furthermore, Authorised Entities should **report significant weaknesses or deficiencies** of the screening system to the management body and take corrective

[2] *As defined within the FATF Assessment Methodology-2022 (Pg. 186)*

measures without delay. Authorised Entities are expected to **keep abreast with any developments by the Sanctions Monitoring Board** including any guidance, notices, decisions, recommendations, and/or rulings.

3.5. Artificial Intelligence

AI adoption within CFT, CPF and TFS compliance frameworks remains limited and at early-stage across the population, with only 15% of respondents indicating active deployment. Looking ahead, 44% indicated that there are no current plans to adopt AI, 28% envisage implementation beyond the next two years, 17% target adoption within the next two years while 11% of respondents are planning to implement AI within the next 12 months.

Among the small cohort that have implemented AI, the prevailing subset of AI is machine learning, with one respondent also reporting reliance on big-data technologies. Reported features cluster around AI-enabled adverse-media screening to support the classification of results, AI-powered anomaly detection including the identification of deepfakes and synthetic identities, and post-transaction analytics to augment traditional monitoring. Integration patterns vary with 67% of respondents having embedded AI within their core banking and/or transaction-monitoring systems, while 33% have not integrated AI into these systems. Among the AI-adopters, 67% indicated that they assign performance monitoring to external vendors, while 33% indicated that they delegate oversight to the Compliance function.

Supervisory Expectations

In line with the UN's Non-Binding Guiding Principles on Preventing, Detecting and Disrupting the Use of New and Emerging Financial Technologies for Terrorist Purposes, also known as the Algeria Guiding Principles, Authorised Entities are encouraged to make optimal use of new and emerging financial and regulatory technologies to contribute to the effective implementation of AML/CFT measures. Technology should be **used responsibly** to facilitate data collection, processing and analysis and help to identify and manage TF risks more effectively and closer to real time. Authorised Entities are **to conduct their own risk assessments prior to** the launch of new products, business practices or the use of new or developing technologies and taking appropriate measures to manage and mitigate those risks, as outlined in FATF Recommendation 15.

Authorised Entities that have and/or are planning on deploying AI must be able to **demonstrate a clear understanding** of the system's design, functionality and limitations, including how the system maintains an audit trail of alerts raised. This is in adherence with the FIAU's Implementing Procedures. In line with Article 76 of the upcoming AML Regulation, Authorised Entities are also expected to **uphold all safeguards relating to information and documentation** obtained in the performance of customer due diligence. The Regulation also expects Authorised Entities to adhere to **meaningful human intervention**, as human oversight ensures that decisions are accurate, appropriate and justified. Consequently, Authorised Entities are also expected to provide transparency, to be able to explain how AI based decisions are made. This is also in line with the Algeria Guiding Principles.

In line with the Algeria Guiding Principles, as financial technologies continue to evolve, Authorised Entities are expected to **strengthen independent oversight** and accountability mechanisms. Independent assurance (whether this is conducted

through an Internal Audit Function and/or any other function responsible for the monitoring of the system's effectiveness) should **periodically verify that results remain effective, fair, and consistent with policy**, and that any model updates or data changes are documented and explainable. Equally, data that is being fed into AI models should be demonstrably fit for purpose through the adoption of ongoing checks to ensure lineage, completeness, accuracy, timeliness, deduplication, and enrichment.

Authorised Entities are reminded that in line with Article 28(3) of the Digital Operational Resilience Act ("DORA") and MFSA Policies specifically, Banking Rule BR/14 on Outsourcing by Credit Institutions Authorised under the Banking Act 1994, Authorised Entities in scope of DORA are required to submit AX50 – Authorisation Form before they enter into a contractual arrangement with an ICT Third-party Service Provider who will be providing an ICT Service that is going to support any of the Authorised Entities' critical or important functions. Authorised Entities in scope of DORA are also required to submit their Register of Information where inter alia, it contains information in relation to contractual arrangements with their ICT third-party providers.

3.6. Training and Awareness

Across the population, Authorised Entities reported delivering a comprehensive suite of annual, induction, and ongoing training through a blended approach combining e-learning modules with in-person, instructor-led sessions. Many respondents indicated the use of detailed case studies, deep-dive discussions on red flags and emerging typologies, and targeted refreshers on STR identification and escalation processes to strengthen staff knowledge and awareness. Board of directors and

senior management are likewise provided training on regulatory developments and evolving financial crime risk landscapes, including emerging sanctions-evasion methodologies.

Supervisory Expectations

In line with the FATF's Guidance for a Risk-Based Approach for the Banking Sector, Authorised Entities are expected to **maintain a risk-sensitive and role-specific training framework** that ensures all employees, particularly those in higher-risk functions, receive ongoing, substantive training proportionate to their exposure to ML and TF risks. Accordingly, Authorised Entities are expected to provide AML, CFT, CPF and TFS' training that is **high-quality**, **relevant** to their specific risk exposure, **aligned** with business activities, and **regularly updated** to reflect current legal and regulatory obligations.

Training should go **beyond theoretical instruction** and incorporate practical elements such as sector-relevant case studies, red-flag indicators, typology analysis, and clear guidance on STR identification and escalation pathways to demonstrate effective, real-world application of anti-money laundering and CFT obligations. The FATF further requires that **training is ongoing** rather than one-off, in line with international standards, and complemented by timely dissemination of relevant updates.

Board of directors and senior management are also expected to receive structured, timely briefings and training that enable them **to understand their governance responsibilities and the evolving ML, TF, PF and TFS evasion landscape**. The visible and active engagement of senior staff in training sends a strong signal about their commitment to the process. Training outcomes should be documented, monitored,

and used to inform continuous improvement, with particular focus on areas where previous deficiencies, thematic findings, or supervisory guidance indicate heightened risk.

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 Maltese-licenced Credit Institutions.

The observations outlined herein indicate that while a number of sound practices are already embedded, there remains aspects of CFT, CPF and TFS' compliance frameworks which would benefit from further strengthening to ensure full alignment with supervisory expectations. In this regard, the expectations being communicated presents several opportunities for Authorised Entities to consider and ultimately improve their CFT, CPF and TFS' frameworks across the sector.

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 letter may inform the Authority's future outcomes-based supervision in the area of Financial Crime Compliance. Authorised entities should use this guidance as an opportunity to assess and strengthen their CFT, CPF and TFS' frameworks, ensuring they meet regulatory expectations.

The MFSA extends its appreciation to all Maltese-licensed Credit 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. The MFSA remains committed to providing ongoing guidance to support best practices and enhance governance and compliance standards.

Yours Sincerely,

Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)
Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2026.06.18 18:25:52 +02'00'

Christopher P. Buttigieg
Chief Officer Supervision

Matthew Scicluna
Digitally signed by Matthew Scicluna
Date: 2026.06.17 08:43:39 +02'00'

Matthew Scicluna
Head, Financial Crime Compliance