
TO : **Regulated Entities**

- i. Crypto Asset Service Providers**
- ii. CIFs**
- iii. UCITS Management Companies**
- iv. Internally managed UCITS**
- v. AIFMs**
- vi. Internally managed AIFs**
- vii. Internally managed AIFLNP**s
- viii. Companies with sole purpose the management of AIFLNP**s
- ix. Small AIFMs under Law 81(I)/2020**

FROM : **Cyprus Securities and Exchange Commission**

DATE : **18 March 2026**

CIRCULAR NO. : **C762**

SUBJECT : **FATF Report Targeted Report on Stablecoins and Unhosted Wallets**

With this Circular, the Cyprus Securities and Exchange Commission (the 'CySEC') wishes to draw the attention of the Regulated Entities the following:

On March 3, 2026, the Financial Action Task Force (the 'FATF') published a report entitled '[FATF Report Targeted Report on Stablecoins and Unhosted Wallets](#)' (the 'Report'). The Report identifies and analyses of illicit finance risks linked to criminals' misuse of stablecoins, particularly through peer-to-peer (P2P) transactions via unhosted wallets. It further sets out recommended actions for countries and the private sector aimed at enhancing existing controls to safeguard the integrity of the financial system.

The Report, highlights how stablecoins' price stability, liquidity and interoperability support their legitimate use while at the same time rendering them attractive for criminal misuse. Such misuse includes their use by money launderers and terrorist financiers, as well as by state-linked cybercriminal groups, including those linked to the DPRK, which have increasingly adopted stablecoins as a preferred method for laundering proceeds from ransomware, phishing and other cyber-enabled crimes. The Report further notes the use of stablecoins by Iranian actors in the context of proliferation financing.

Vulnerabilities include how P2P transactions via unhosted wallets occur directly between individuals or entities, without the involvement of a regulated intermediary Virtual Asset Service Provider (VASP) or financial institution as well as how stablecoin issuers may face difficulties in controlling cross-chain activities, which may therefore fall outside counter-illicit finance controls.

In addition, good practices to mitigate the misuse of stablecoins and case studies demonstrating how new technologies and blockchain analytical tools, along with other risk mitigation measures, have been used to detect and disrupt illicit activity involving stablecoins, are highlighted.

CySEC would like to point that in line with the [FATF's 2021 Updated Guidance for a RiskBased Approach to VASPs](#), Regulated Entities are expected to adequately identify, assess and mitigate the risks associated with the use of stablecoins and unhosted wallets.

Furthermore with regards to the **EU Regulation 2023/1113 - Transfer of Funds Regulation** where obligations were circulated to the Regulated Entities via [C675](#). In this regard, paragraph 71 of the Report highlights that the FATF has issued guidance on best practices for VASP supervision in its report entitled “Best Practices for Travel Rule Supervision”. These practices are also applicable to supervisors overseeing stablecoin issuers and other obliged entities participating in stablecoin arrangements.

The CySEC urges Regulated Entities to duly take into account the afore-mentioned FATF’s report and to consider the specific money laundering and terrorist financing risks that may arise from such arrangements. In particular, Regulated Entities are expected to enhance their understanding of the risks associated with stablecoins and unhosted wallets transfers and to enhance their risk-based approach under the Prevention and Suppression of Money Laundering Activities Law (L. 188(I) 2007) as amended from time to time.

Sincerely,

Dr George Theocharides
Chairman, Cyprus Securities and Exchange Commission