To:
Malta Financial Services Authority
Triq l-Imdina
Zone 1, Central Business District
Birkirkara CBD 1010
Malta

For the attention of the Chief Executive Officer and the Chief Officer Supervision

Cc: European Banking Authority, Paris

For the attention of:
Marilin Pikaro
Director, Innovation, Conduct and Consumers
European Banking Authority

Cc:
Rūta Merkevičiūtė
Head of Unit, Digital Finance
Ruta.Merkeviciute@eba.europa.eu

EBA-MiCAR-Supervision@eba.europa.eu

Date: 24 August 2026
Our reference: EFRI/MFSA/StablR-02

Enclosures:
(1) EFRI letter to the MFSA of 8 July 2025
(2) MFSA letter to EFRI of 1 August 2025
(3) EFRI Payvision Report of 15 May 2026

Subject: StablR Ltd – renewed request for supervisory review following the May 2026 cyber incident, the continuing suspension of redemption, and new evidence concerning the Payvision management environment

Dear Sir or Madam,

EFRI – the European Funds Recovery Initiative – is a non-profit victim-protection organisation included in the European Commission's list of qualified entities designated for cross-border representative actions pursuant to Directive (EU) 2020/1828. We act for consumers harmed by online investment and payment fraud.

We state at the outset that EFRI does not act for any identified holder of EURR or USDR. This submission is made in the public interest and on the basis of EFRI's direct and continuing involvement with victims of the Barak and Lenhoff fraud networks, for which Payvision B.V. provided payment infrastructure. Every factual assertion below is either publicly documented or drawn from criminal-file material reviewed by EFRI. We are willing to make the underlying documents available to the MFSA on request.

On 8 July 2025, EFRI asked the MFSA to reassess StablR Ltd's licence, including the fitness and properness of its senior management and its ultimate beneficial ownership, in light of the Payvision management history. By letter dated 1 August 2025, the MFSA stated that it was "currently undertaking an exhaustive analysis of the contents of the letter and any implications on the relevant licensed entity", invited EFRI to a meeting and copied the European Banking Authority. EFRI declined a non-public meeting, stating that, given the public-interest nature of the matter, we would address it publicly and in writing. We specifically urged the MFSA to obtain and review the DNB supervisory report sent to Payvision on 5 September 2020 for the fit-and-proper assessment. Although EFRI stated that it intended to submit further written material within 21 days, no further substantive submission was made at that stage. We have not been informed of the outcome of the MFSA's announced analysis.

We write again because two material developments have since occurred. First, StablR has suffered a cyber incident raising serious questions about controls governing the creation of monetary liabilities without corresponding backing. Second, EFRI has obtained and analysed substantially more extensive Payvision criminal-file material, forming the basis of our report of 15 May 2026 and materially strengthening the concerns raised in July 2025. We ask the MFSA to consider both developments in the context of the supervisory analysis announced in August 2025.

1. The cyber incident and the core issuance controls

On 25 May 2026, StablR confirmed that unauthorised access had affected its platform infrastructure, suspended minting and redemption, and acknowledged that:

> "*the circulating supply of USDR and EURR tokens is currently not fully backed at the 1:1 ratio required under MiCAR.*"

The incident occurred on 24 May 2026. On 29 May 2026, StablR activated its Recovery Plan, stating that the safeguarded assets backing EURR and USDR before the incident remained intact, and that exchanges had been asked to suspend trading, deposits and withdrawals in both tokens.

According to Blockaid[1], as reported by *The Block* on 24 May 2026, the attacker minted approximately 8,350,000 USDR and 4,500,000 EURR, with a reported aggregate face value of approximately USD 13.5 million, without corresponding reserves. Roughly USD 10.4 million in face value was subsequently swapped for ETH across decentralised exchanges. Blockaid attributed the incident to the compromise of one private key in a minting multisig configured with a **1-of-3 signature threshold** and described the failure as a governance and key-management issue rather than a flaw in the smart-contract code.

We have not identified any subsequent technical post-mortem published by StablR confirming or correcting that analysis or quantifying the remaining shortfall. **If Blockaid's account of the 1-of-3 configuration is correct, compromise of a single authorised key was sufficient at the minting-authority level. Dual approval was therefore not required for that critical function.** This raises obvious questions concerning key management, segregation of duties, independent authorisation of issuance, and controls linking token issuance to corresponding funds.

We therefore ask whether the MFSA has examined:

- the reported 1-of-3 threshold on the minting authority;
- segregation of duties and independent authorisation of token issuance;
- controls preventing minting without corresponding funds;
- transaction limits, anomaly detection and private-key governance; and
- whether the pre-incident control environment complied with MiCAR, DORA and the conditions under which StablR was authorised.

2. The published white paper and Article 51(12) MiCAR

StablR's crypto-asset white paper for EURR, version 3.2 dated 2 December 2025 and still published on the issuer's website, states:

> *"StablR will guarantee at all times that all StablR Euro (EURR) are fully backed with fiat, fiat equivalent or other secure low risk investments at a rate of 1 EURR : 1 Euro."*

and:

[1] https://x.com/blockaid_/status/2058378832684405245?

> *"The holders of StablR Euro (EURR) have a right of redemption at any time and at par value … The Issuer shall, following redemption, process the payment back to the holder within twenty-four (24) hours."*

Since 25 May 2026, StablR's own statement that its circulating supply is not fully backed has been inconsistent with the first representation, while the continuing suspension prevents holders from exercising the redemption right described in the second.

Article 51(12) MiCAR requires any significant new factor, material mistake or material inaccuracy capable of affecting the assessment of an e-money token to be described in a modified crypto-asset white paper, notified to the competent authority and published on the issuer's website.

A material backing shortfall and a suspension of redemption lasting several months appear plainly capable of affecting the assessment of the tokens and therefore appear to engage Article 51(12).

We therefore ask:

Has StablR notified the MFSA of a modified white paper for EURR and/or USDR, and has such modified white paper been published? If not, on what basis does the MFSA consider Article 51(12) not to be engaged?

Unlike the other matters raised in this letter, this concerns a state of affairs that is verifiable today and, if uncorrected, is continuing.

3. Three months of suspended redemption

Article 49(4) MiCAR provides that, upon request by a holder, the issuer *"shall redeem it, at any time and at par value"* by paying the monetary value of the e-money token held. Article 49(6) provides that redemption shall not be subject to a fee, without prejudice to Article 46.

Article 46, applicable to e-money-token issuers mutatis mutandis pursuant to Article 55, permits a recovery plan to include suspension of redemptions as a recovery option under Article 46(1)(c). Separately, Article 46(4) gives the competent authority power temporarily to suspend redemption where justified having regard to the interests of token holders and financial stability.

EFRI does not dispute that suspension may form part of a lawful recovery response. Our concern is the legal and supervisory basis for **its continuation for three months**. No current shortfall figure, timetable for restored redemption or partial-redemption mechanism has been published.

We therefore ask:

- Has the MFSA made a determination under Article 46(4) MiCAR in respect of EURR and USDR? If so, when was it made and what conditions govern its continuation?
- If the suspension rests solely on StablR's Recovery Plan under Article 46(1)(c), how has the MFSA assessed its continued use against the statutory redemption right in Article 49(4)?
- Will the MFSA, insofar as legally permissible, make a public statement clarifying the legal basis and current status of the suspension for token holders?

4. Recovery plan or redemption plan?

Article 47 MiCAR, likewise applicable pursuant to Article 55, provides for implementation of an orderly redemption plan upon a decision by the competent authority that the issuer is unable or likely to be unable to fulfil its obligations.

The EBA Guidelines on redemption plans (EBA/GL/2024/13, paragraphs 83–86) require the competent authority to make a comprehensive assessment of that question. Importantly, the Guidelines expressly distinguish between EMT issuers subject to a MiCAR requirement to hold a "reserve of assets" and EMT issuers that are not subject to that requirement unless the competent authority has imposed it. EFRI therefore does not suggest that the guideline indicator "*having the reserve of assets lower than liabilities*" automatically or necessarily applies to StablR.

The relevant question is whether, under the requirements applicable to StablR, it is unable or likely to be unable to fulfil its obligations. StablR's own acknowledgement that its circulating supply is not fully backed, together with the continuing non-availability of redemption, is plainly material to that assessment.

We therefore ask:

- Has the MFSA assessed whether StablR is unable, or likely to be unable, to fulfil its obligations within the meaning of Article 47 MiCAR and whether the redemption plan should be implemented?
- Has the MFSA considered whether partial or pro-rata redemption could lawfully and operationally be implemented from available assets while ensuring equitable treatment of token holders?

Holders currently have no public information about the assets available to meet redemption claims, the size of the remaining shortfall, recoveries, additional committed funding or the timetable for restoring redemption. Three months into the suspension, greater transparency is warranted.

5. The platform is owned outside the licensed entity – with overlapping directors

StablR's regulatory documentation states that *"STB Software Development B.V. owns the IT and the platform."* STB is a Dutch group company and is not the licensed issuer.

According to the same white paper, Gijs op de Weegh and Corné van der Meijden are directors of STB Software Development B.V. and also directors of StablR Ltd. Both are also directors of Plutus B.V. Robin Nijkamp is listed as a director of STB Software Development B.V.; the white paper does not list him as a director of StablR Ltd.

The relevant point is not that the technology therefore sits "outside the regulatory perimeter". Rather, the platform is owned by an unlicensed related undertaking while regulatory responsibility for StablR's ICT risk remains with the licensed entity. DORA does not exclude intra-group ICT arrangements: intra-group ICT service providers and their contractual arrangements must be included in the relevant ICT third-party-risk framework and register of information.

We therefore ask whether the MFSA has examined:

- whether the ICT services provided by STB Software Development B.V. support a critical or important function, and whether the arrangement is included in the register of information required by Article 28(3) DORA;
- if the services support a critical or important function, whether the enhanced contractual requirements of Article 30(3) DORA are satisfied, including appropriate access, inspection and audit rights and exit arrangements;
- how conflicts of interest arising from the overlapping directorships are managed and what role StablR's non-executive directors, including its Independent Non-Executive Chairman, played before and after the incident;
- whether StablR submitted the notifications and reports required under Article 19 DORA and the applicable reporting rules within the prescribed deadlines; and
- the allocation of responsibility between StablR Ltd and STB Software Development B.V. for the key-management failure reported by Blockaid.

6. New evidence concerning the Payvision management environment

On 15 May 2026, EFRI published a detailed report based on an extensive review of criminal files, payment records, contracts, internal communications and investigative material concerning the fraud organisations operated by Gal Barak and Uwe Lenhoff. It includes evidence from the Saarbrücken proceedings that was not available to EFRI in earlier civil proceedings.

Those structures affected more than 60,000 European consumers and caused losses of approximately EUR 340 million. Many victims continue to pursue compensation today; civil proceedings and collective recovery efforts remain ongoing. **For them, Payvision is not a historical matter.**

The report documents that Payvision and Acapture provided extensive payment infrastructure to the Barak and Lenhoff structures. According to Payvision's own figures reproduced in the criminal files, approximately EUR 77.7 million in card payments were processed for Barak-related platforms and approximately EUR 55.6 million for Lenhoff-related platforms. Thousands of chargebacks and fraud reports and 273 SAR/FIU filings concerning the relevant entities are documented, alongside repeated regulatory warnings and internal compliance concerns.

Of particular relevance is the documented sequence concerning Gpay Ltd. Payvision's compliance function raised serious concerns in early 2018. Transactions were subsequently blocked following further warnings. The accounts were then released, a new agreement (signed by Gijs op de Weegh) was concluded in July 2018, and more than EUR 37 million was processed for Barak-related platforms thereafter.

The significance of that sequence is not that EFRI can attribute each subsequent decision to a particular individual. It is that the risk had been detected and escalated, yet business with the relevant counterparty subsequently resumed. That is directly relevant to supervisory questions concerning management judgement, escalation procedures and risk culture.

7. The position of Gijs op de Weegh

StablR's Chief Executive Officer and director, Gijs op de Weegh, was not merely a former employee of Payvision. The criminal-file material reviewed by EFRI documents that he co-founded Payvision, held senior operational management functions and signed merchant agreements with entities used for the Lenhoff and Barak platforms.

Corné van der Meijden, StablR's Chief Risk and Operations Officer and director, previously served as Payvision's Chief Financial Officer.

The relevant test here is the MFSA's own continuing fit-and-proper framework for financial institutions. FIR/02/2025 provides that directors, controllers and officers must be fit and proper and conduct business with integrity and skill, and expressly refers, when assessing competence, to soundness of judgement, diligence and experience of similar responsibilities.

The absence of a criminal sanction against Mr op de Weegh in the Netherlands for the Payvision case does not substitute for that supervisory assessment. According to the material reviewed by EFRI, the Dutch investigation did not obtain the Austrian and Saarbrücken criminal files.

The issue for the MFSA is therefore not criminal liability, but whether all information now available is relevant to the continuing fitness and properness assessment of persons managing a regulated financial institution.

8. Why both matters warrant renewed assessment

EFRI does not assert that the May 2026 cyber incident was caused by the previous Payvision activities of StablR's management. No such assertion is necessary.

The two matters are relevant for a more limited but important reason. At Payvision, the criminal-file record documents risk signals and compliance escalation followed by the resumption of business with the relevant merchants. At StablR, if Blockaid's analysis is correct, the minting architecture permitted compromise of a single authorised key to result in administrative control and the creation of unbacked tokens.

These are different events and one does not prove the other. Both, however, raise legitimate supervisory questions concerning the effectiveness of controls, management oversight, risk culture and soundness of judgement.

The regulatory question is therefore whether the actual roles, responsibilities and management environment of StablR's senior management at Payvision were adequately considered when StablR was authorised and in the MFSA's 2025 analysis, and whether the evidence published in May 2026, together with the subsequent StablR incident, requires that assessment to be revisited and updated.

9. Action requested

EFRI respectfully requests that the MFSA:

- confirm whether the "exhaustive analysis" announced in the MFSA's letter of 1 August 2025 was concluded; whether, as specifically requested by EFRI in August 2025, the MFSA obtained and considered the DNB supervisory report sent to Payvision on 5 September 2020 or otherwise obtained the relevant findings from DNB; and whether the May 2026 Payvision Report and the subsequent StablR incident have caused that assessment to be reopened, supplemented or updated;
- determine and, insofar as legally permissible, clarify publicly the legal basis and current status of the continued suspension of EURR and USDR redemption and whether the conditions for implementation of the redemption plan under Articles 47 and 55 MiCAR are met, including whether partial or pro-rata redemption can lawfully be implemented;
- require StablR to publish a modified crypto-asset white paper under Article 51(12) MiCAR, or state why the MFSA considers that provision not to be engaged;

- conduct, or where appropriate update, a fitness-and-properness assessment of the relevant members of StablR's management body taking into account EFRI's report of 15 May 2026 and the additional Austrian and German criminal-file material underlying it;
- assess whether StablR continues to satisfy the conditions on which its licence was granted, including Article 6(1)(d) and (i) of the Financial Institutions Act and, if the Authority determines that StablR has insufficient assets to cover its liabilities, Article 6(1)(j); and
- confirm whether the questions concerning ultimate beneficial ownership and qualifying shareholdings raised in EFRI's letter of 8 July 2025 have since been assessed, including in relation to changes in shareholdings after that date.

10. Response and next steps

EFRI represents consumers who continue, years later, to bear the consequences of the financial infrastructure supplied to the Barak and Lenhoff schemes. Where individuals who held senior functions in one regulated financial institution subsequently manage another, the fit-and-proper regime can only serve its purpose if the supervisor examines the substance of that previous management history and takes account of significant new information emerging after authorisation.

The StablR cyber incident and the substantially enlarged evidentiary record concerning Payvision are two separate and compelling reasons to revisit and update the supervisory analysis announced by the MFSA in August 2025.

We remain available to provide the MFSA with the underlying documentary material at any time and would appreciate a substantive response addressing the matters raised above.

Yours faithfully,

Elfriede Sixt
Chairwoman
EFRI – European Funds Recovery Initiative