Swiss Fintech Alliance (SFA)
Via Redondello 24a
CH - 6982 Agno

Eidgenössisches Finanzdepartement EFD

Staatssekretariat für internationale Finanzfragen SIF
Frau Melanie Friedli
Herr David Rieder
Bundesgasse 3
3003 Bern

Per Mail to:
melanie.friedli@sif.admin.ch

Agno, 16 September 2026

Subject: SFA feedback on the proposed amendments to the Anti-Money Laundering Act

Dear Ms Friedli,
Dear Mr Rieder,

Thank you again for giving us the opportunity to comment on these proposals at an early stage. We understand that these are internally discussed, non-final proposals, and we have framed our comments accordingly — as drafting input on the two considerations sketched, rather than as a formal consultation response.

We support the objective of strengthening the Swiss AML/CFT framework and of establishing technologically neutral and proportionate rules for traditional and virtual assets.

A note on priority, before the sections that follow. Of everything below, two points matter most. First, the value threshold at which Travel Rule identification and customer due-diligence obligations apply should be raised to a level that makes a practical difference — not CHF 500, which in practice changes very little (Section 3), but a materially higher figure such as CHF 5,000 or CHF 10,000. Below that level, identification requirements mainly push activity into fully unhosted, peer-to-peer transfers that no regulator can see at all. Second, the freeze/reporting mechanism for virtual-asset and stablecoin transactions should mirror the architecture that already governs fiat under Art. 9a, 9b and 10 GwG — no continuous freeze while MROS analyses a report, a defined point at which the issuer may lift the measure if MROS stays silent — for an issuer the analogue is lifting the measure or redeeming against a traceable payout, since it cannot terminate a secondary-market holder it never onboarded, and a short, capped freeze only once MROS actually forwards a case to a prosecution authority — not a separate, stricter, open-ended crypto-specific regime (Sections 6 and 7). Where an address is on a sanctions list or on a list communicated under Art. 22a GwG, an immediate freeze remains appropriate, as it is today.

One general observation, offered as context for the drafting comments that follow. Alignment with EU rules does not of itself give Swiss providers access to the EU market, so a Swiss rule that is as strict as or stricter than its EU counterpart carries a cost without a corresponding benefit. Where the proposals go beyond the FATF Standards — as the CHF 500 threshold and the freeze-first holding regime do — we would ask that the additional stringency be justified on its own terms.

We would ask SIF to weigh each proposed rule against two tests: does it reduce AML/CFT risk, and does it leave Switzerland an attractive place to run a regulated fintech business? Make the regulated Swiss route materially more cumbersome than a self-hosted wallet or an offshore provider, and customers migrate there instead — which would hurt Swiss competitiveness without helping AML/CFT, since it pushes activity away from the institutions that can actually be supervised.

1. Scope of the Travel Rule

The explanatory text refers to “transfers of assets for payment purposes”, whereas the proposed statutory wording refers to:

« Lors de transferts de valeurs patrimoniales ayant cours de paiement ou d’actifs virtuels. »

Read literally, this wording supports two different readings: narrowly, as covering only transfers of assets that serve a payment purpose, whether fiat or virtual; or broadly, as covering any transfer of virtual assets at all, payment-related or not, given the disjunctive “ou”. We think the explanatory text’s own framing — “transfers... for payment purposes” — points to the narrower reading, and that this is also the more workable one in practice, for the reasons set out below. We would ask that the final statutory wording remove this ambiguity directly, rather than leave it open to interpretation.

Before turning to virtual assets, one point on the provision itself. It is technology-neutral by design: it lifts the existing duties of Art. 10 GwV-FINMA for payment orders to the level of the statute, for all transfers of assets recognised as means of payment — fiat included. SIF’s explanatory note says so: the effects reach circles not directly affected by the FINIG revision. For the payment-service, e-money and card providers among our members this is the operative change. A duty at statute level is harder to adapt as transmission standards evolve; SRO-supervised intermediaries are brought within it; and low-risk exemptions would be designated by five separate bodies — FINMA, CFMJ, DFJP, OFDF and the SROs — with no coordination mechanism, and with no effect on a foreign counterparty.

We ask, first, that the data to be transmitted be specified by ordinance, not exceed the elements carried by SIC, SEPA and SWIFT messages, and remain those applicable under Art. 10 GwV-FINMA on 1 January 2027 until amended — so that the statutory change and the ordinance revision are one implementation, not two — and that a virtual IBAN or reference attributable to an identified account holder count as an account identifier; second, that the provision for a single intermediary apply only where the counterparty’s assets are not held with a financial intermediary, and never to transfers between clients of one institution; third, that card-initiated payments for goods and services, where the card number accompanies the transfer, be excluded as under Recommendation 16, and that other low-risk exemptions be designated in one list binding all intermediaries rather than by five bodies; and fourth, that the term « valeurs patrimoniales ayant cours de paiement » be reconciled with the explanatory note, which speaks of book money, and that it be made clear where e-money tokens and tokenised deposits sit relative to « actifs virtuels ».

We think the right test for scope is whether the transaction is a payment order in the technical sense, not the type of asset or counterparty involved. A payment order is an instruction from a customer to a financial intermediary to pay an amount to a beneficiary the customer designates, via another (or the same) financial intermediary. A purchase order — for example, an instruction to a crypto institution to buy Bitcoin on the customer's behalf — is not a payment order, even though it involves a movement of value: the customer is not designating an external beneficiary and receives the purchased asset themselves. Self-contained transactions of this kind — a purchase, exchange, or investment order — should remain outside the Travel Rule's scope, just as they are today for fiat instruments and securities: a customer does not trigger third-party identification by calling their bank and placing a stock order. For the avoidance of doubt, the exclusion should be defined by the absence of a transfer to an address outside the institution, not by the label of the order: an order executed by moving the customer's assets to an external address is a transfer within Recommendation 16 whatever it is called — while transfers between a customer and the customer's own external wallet are not transfers to a third party and should be carved out expressly.

Where a customer receives an amount from an external third party or sends an amount to an external third party they designate as beneficiary, above the threshold discussed in Section 3, we think information on that third party should be obtained — and the transfer attributed to our customer. This is the Travel Rule's proper function: ensuring a financial intermediary knows who its customer is transacting with outside the institution, which is as much a sanctions and counter-terrorist-financing (CTF) safeguard as an anti-money-laundering one.

We ask that the statutory wording reflect this distinction precisely: the obligation should attach to payment orders between our customer and an identifiable external third party, above the threshold set out in Section 3, and should not extend to self-contained purchase, exchange or investment orders that a customer places for their own account.

2. Transactions involving self-hosted wallets and DeFi

The same distinction applies here: where a self-hosted wallet or a DeFi protocol is simply the venue for a customer's own purchase or exchange order, with no external beneficiary designated, Section 1's reasoning applies and no Travel Rule obligation should arise.

We would also ask SIF to reconsider the additional proof-of-control step that FINMA guidance currently applies to deposits from, and withdrawals to, a customer's own external wallet (the so-called "Satoshi test"). This is not required by the FATF standards; it is a Swiss-specific practice. We note that the EU's Transfer of Funds Regulation does require verification of ownership for transfers to or from a self-hosted address above EUR 1,000. A threshold- and risk-based version — verification only above CHF 1,000 or where risk indicators are present, by any reasonable method including a signed message or a self-declaration in lower-risk cases — would align Switzerland with that benchmark while removing the step for the low-value, own-wallet transfers where it serves no purpose.

Where a transaction genuinely does involve an external third party — a transfer to or from another person's self-hosted wallet, for instance — we think the obligation should be to obtain information on the counterparty and, on a risk basis, to establish its control over the wallet — the standard the available tools can actually meet, since blockchain analytics attribute an address to an entity or a risk category rather than identify a person.

The baseline matters here. Under FINMA's guidance of 26 August 2019, a transfer to or from a wallet belonging to a third party is possible only if the institution has first identified the third party as it would a client, established the beneficial owner and proven the third party's ownership of the wallet by technical means — a bar so high that in practice institutions decline such transfers and clients route them through their own wallets instead. The proposed provision for transfers involving only one financial intermediary codifies that practice at statute level and adds relief below CHF 500. Its practical value therefore turns entirely on the standard it sets: if lit. b keeps the 2019 bar — identify a stranger as one would a client — the path stays closed in practice; if it is framed as obtaining information and establishing control over the wallet, it becomes usable and brings within the regulated perimeter activity that today is pushed to foreign or unregulated providers. The provision also gives the 2019 guidance the statutory basis that has been questioned in practice, which we welcome.

On the wording of that provision we ask for three changes. Lit. b, « s'assurer de l'identité de cette contrepartie », sets a standard an intermediary cannot meet for a counterparty with which it has no relationship, and goes beyond SIF's own explanatory note, which states that only the obtaining of information is regulated and not the due-diligence duties of Art. 3–7 GwG. The verb should be « obtenir », with risk-based plausibility checks specified at ordinance level. Lit. c, « le pouvoir de disposition de cette contrepartie sur les valeurs patrimoniales à transmettre », describes only an incoming transfer; for an outgoing transfer what is verified is control over the destination address, and for a cash transaction the recipient has no power of disposal over anything yet. The provision should state which direction it addresses and how, if at all, it applies outside virtual assets. Finally, the draft anchors the duty to transmit but not the beneficiary institution's duty to act on incomplete information, which today sits in GwV-FINMA; both halves should move together, and the statute should provide a procedure for incoming transfers with missing or incomplete information — risk-based acceptance, hold, request or return, without an obligation to return on-chain — and a transition period for counterparties that cannot yet transmit.

For interactions with DeFi protocols specifically, we would caution against a blanket identification requirement. In most cases, the counterparty to a DeFi interaction is a smart contract or a liquidity pool, not an identifiable natural or legal person, and cannot be identified with reasonable effort even using the analytics tools available today. DeFi's on-chain transparency already provides meaningful traceability that those tools can draw on where needed; the right response to that is not to require an identification that generally cannot be performed. A rule that in practice prevents financial intermediaries from facilitating customer access to DeFi protocols would be disproportionate and not technology-neutral and would push this activity toward unsupervised channels — increasing risk rather than reducing it. FATF's July 2026 Targeted Report on Decentralised Finance itself frames DeFi arrangements as falling within Recommendation 15 where a person exercises control or sufficient influence over the arrangement; we think that same control-based, functional test is the right starting point domestically — where no such person exists, a blanket identification duty is neither workable nor proportionate. We would encourage a framework that gives financial intermediaries workable incentives to intermediate DeFi activity for their customers, rather than one that makes this impractical. Two questions should nonetheless be kept apart: whether a DeFi arrangement is itself a VASP, which is the control-based question the FATF report addresses, and whether a Swiss institution's transfer of a customer's assets to a contract address is a transfer for the purposes of the information duties — which it is. The workable answer to the second is not a list of designated protocols — no exemption body will maintain one — but a rule that where the counterparty is a contract with no identifiable person behind it, the institution documents its own due diligence on the protocol and the information duty is deemed satisfied.

As with Section 1, we consider the more productive lever to be the value threshold at which identification obligations apply (Section 3), rather than the nature of the wallet or protocol involved.

3. CHF 500 threshold

The proposed CHF 500 threshold strikes us as particularly low.

FATF Recommendation 16 — reconfirmed in the June 2025 revision on payment transparency, and applied to virtual-asset transfers through Recommendation 15 — allows a de minimis threshold of no higher than USD/EUR 1,000, below which only the names of originator and beneficiary and an account or transaction reference need accompany the transfer, unverified unless there is suspicion. That is precisely the structure of the proposed al. 2. The proposal adopts the FATF architecture and halves the FATF figure, without a stated reason. The EU's Transfer of Funds Regulation applies EUR 1,000 to fiat transfers. The question is therefore why Switzerland should set a materially lower bar than both.

Neither the sanctions/CTF objective underlying the Travel Rule (Sections 1–2) nor the GwG anti-money-laundering objective is served by a threshold this low. A CHF 500 threshold mainly burdens the general public and ordinary wallet operators with identification requirements for low-value, low-risk transfers, while doing little to capture the transaction sizes at which laundering or sanctions evasion actually occurs. In practice, thresholds set this low are rarely used as intended: avoiding them requires smurfing-prevention monitoring that is itself more burdensome than simply identifying the counterparty, so the exemption goes largely unused and changes little in practice. At the same time, an unrealistically low threshold pushes ordinary users toward fully unhosted, peer-to-peer transfers that fall outside any regulated channel and remain completely invisible to supervision — the opposite of the intended effect.

The practical consequences matter more than the number itself. A very low threshold creates disproportionate technical and operational burden for ordinary, low-value transactions, and pushes users of regulated Swiss solutions toward self-hosted or foreign alternatives instead.

A significantly higher threshold would serve the same AML/CFT objective without that side effect.

We ask that the proposed threshold be reconsidered on risk-based, proportionality and competitiveness grounds, and set at a level — CHF 5,000 or CHF 10,000 — that will actually be used in practice. Should SIF wish to stay within the ceiling of USD/EUR 1,000 that Recommendation 16 sets for a de minimis threshold, we note that this ceiling concerns only the data set to be transmitted with a transfer. It does not extend to the verification of a counterparty's identity and control over a wallet under the one-intermediary provision (al. 1 let. b and c), which the FATF Standards leave to each country's risk-based judgment; that threshold Switzerland is free to set, and it is where the burden lies.

4. A related but distinct point: calibrating customer due-diligence thresholds for virtual assets

This point is separate from the Travel Rule discussed above and should not be read as part of it. Sections 1–3 concern information about a counterparty to a transfer. This section concerns a Swiss institution's due diligence on its own customer — a different obligation under Art. 3 GwG.

Today, that customer due-diligence question is addressed for virtual currencies only by Art. 51a GwV-FINMA, and only outside a standing business relationship. For institutions that maintain a standing relationship with the customer — a wallet account, for instance — no equivalent graduated threshold exists for virtual assets, even though one does exist for fiat-denominated payment instruments under Art. 11 and Art. 12 GwV-FINMA. We think this gap belongs on the table alongside the Travel Rule reform, since both stem from the same underlying question of how Switzerland treats virtual assets under the GwG framework.

We propose a three-tier model, built on the logic already applied to fiat payment instruments:

Tier	Designation	Threshold (cumulative)	Legal basis / benchmark
1	No due diligence	≤ CHF 1,000 (aggregated across connected transactions)	Art. 51a para. 1 and 1bis GwV-FINMA (currently limited to transactions outside a standing business relationship)
2	Customer-provided information, unverified (no ID check, no video/online identification, no residence check)	CHF 1,000 – 5,000 (cumulative)	No dedicated statutory basis for virtual assets today; proposed by analogy to the general low-value waiver principle of Art. 7a GwG, which is technology-neutral in its wording
3	Full identification (Full AML/KYC)	from CHF 5,000	Art. 3 GwG in conjunction with Art. 44–49 GwV-FINMA

Tier 2 rests on the following grounds:

- Art. 7a GwG, the statutory basis for all due-diligence waivers, is framed in technology-neutral language (“assets of low value”, “no indication of money laundering”) and is not limited to fiat instruments by its own wording. Art. 11/12 GwV-FINMA have so far concretised that principle only for fiat payment instruments — a product of when those provisions were drafted, not a deliberate policy choice to hold virtual assets to a stricter standard.
- Equal treatment: a low-value balance in an e-money wallet and an equivalent balance in a stablecoin wallet carry comparable money-laundering risk — arguably lower for the latter, given that on-chain transactions are traceable through blockchain analytics in a way cash and much of e-money are not.
- Swiss law has consistently set the threshold for genuinely risk-relevant transaction monitoring in the six-figure range (Art. 14 para. 3 let. a GwV-FINMA: CHF 100,000; Art. 8a GwG: CHF 100,000). Structuring and layering — the actual mechanics of laundering — operate at that scale,

not at CHF 1,000–5,000, and would in any case still be caught by ongoing transaction monitoring (Art. 20 GwV-FINMA) and the aggregation rule for connected transactions (Art. 51a para. 1bis GwV-FINMA), independently of any onboarding threshold.

- FATF Recommendation 1 asks that compliance effort track risk. Verifying every low-value balance in full does not track risk; it spends the same scrutiny on a wallet holding a few hundred francs as on one holding hundreds of thousands.

We recognise that Tier 2, as outlined, is not yet grounded in a codified provision and would need either a request under Art. 11 para. 5 GwV-FINMA or an explicit statutory clarification. We raise it now because this reform is the natural moment to close the gap — rather than leaving virtual-asset institutions to work from an analogy that neither the industry nor the regulator has formally confirmed.

As an aside re GwV-FINMA: we would appreciate and encourage FINMA to review this part of the ordinance — dating from 3 June 2015 — and simplify it. Nine separate provisions spanning seventeen distinct transaction categories, several with overlapping monthly, annual and rolling-window cumulation rules, strike us as difficult to implement reliably and disproportionately complex relative to any discernible risk-management benefit.

5. Stablecoin blacklist

We support the objective of preventing the misuse of stablecoins for money laundering and terrorist financing, and we view the direction of the proposed approach positively.

As we understand it, a blacklist would attach to individual tokenholders or wallet addresses, not to token types as such. Today, an issuer is in effect expected to treat every tokenholder as requiring identification ("whitelisting") from the outset. The Vorentwurf (Art. 8a para. 3) offers the blacklist as an alternative to that identification route rather than as its abolition: under either route the issuer assesses and monitors secondary-market risk (para. 2) and maintains the technical capability to act (para. 4). Under the blacklist route, a tokenholder would not need to be identified unless and until there are grounds to believe that the tokenholder, or the assets involved, are connected to criminal conduct — at which point that address is blacklisted.

This is, in our view, a meaningful simplification for regulated stablecoin issuers and should be welcomed: it removes the need for blanket upfront identification of every tokenholder, while preserving the ability to act against known bad actors.

We also think it is reasonable to treat all stablecoins representing a claim against a Swiss issuer alike for this purpose — the "monnaie virtuelle couverte" scope in the proposal is not, in our view, too broad a net. Extending the capability requirement itself is consistent with the FATF's Targeted Report on Stablecoins and Unhosted Wallets of 3 March 2026 and with the approach of the US GENIUS Act. The scope should, however, attach to what the issuer technically controls: the duty should be framed as maintaining the capability for tokens the issuer controls, limited to deployments the issuer itself operates rather than bridged or wrapped representations created by third parties — and if immutable designs with no administrative function are thereby excluded from Switzerland, that should be said rather than left to follow from a definition.

The ability to freeze and report should not depend on identifying a natural or legal person behind an address; it should depend on the report being actionable. Identity, attribution to a named custodian to which

a request can be routed, or documented linkage to a predicate offence such as a hack should each suffice. Blockchain-based assets are often traceable to their origin — for instance, funds derived from a hack — well before, if ever, the person behind a wallet is known. A report to MROS can supply valuable leads for law enforcement even without an identified human counterparty, and the blacklist and reporting mechanism should be designed to allow freezing and reporting on that basis.

We would still ask for clarity on:

- the criteria and evidentiary basis for placing an address on the blacklist;
- who makes that determination and how it can be reviewed;
- the practical mechanism by which regulated institutions are expected to implement and maintain the blacklist;
- which lists trigger a mandatory freeze — SECO and UN sanctions designations under the embargo legislation, and lists communicated under Art. 22a GwG — and which are discretionary, such as foreign sanctions lists, whose application at a foreign authority's request raises Art. 271 StGB, and vendor risk lists;
- the distinction between freezing an address, which is reversible, and destroying or re-issuing tokens, which is not: the minimum capability should be the freeze, and destruction or clawback should require a judicial order, as the US framework requires a lawful order;
- the treatment of addresses that hold assets for many persons — liquidity pools, bridges and the omnibus wallets of regulated custodians — where a single freeze immobilises every participant, and where the appropriate step is to notify the custodian of record, which reports and applies its own controls under Art. 9 and 9a GwG at client level and leaves any freeze to MROS's decision; and
- governance of the blacklisting function itself: a mandated freeze capability is a privileged key over third-party property, and key custody, four-eyes control and audit should be addressed alongside the duty.

6. Freeze/block and reporting obligation

We would like to set out how the freeze/reporting mechanism actually works for fiat today, since we think it is the right model for virtual-asset and stablecoin transactions as well — and it is more permissive than the sequence the current proposal appears to contemplate.

Under Art. 9a GwG, while MROS conducts its own analysis of a report (Art. 23 para. 2 GwG), the financial intermediary continues to execute customer orders relating to the reported assets; it is only required to execute orders involving significant assets in a form that preserves traceability for law enforcement. There is, in other words, no continuous freeze during MROS's analysis phase.

A freeze obligation under Art. 10 para. 1 GwG arises only once MROS informs the financial intermediary that it has forwarded the reported information to a prosecution authority (Art. 23 para. 5 GwG) — and even then, the freeze is capped at five working days, pending a ruling from that authority (Art. 10 para. 2 GwG).

If MROS does not inform the financial intermediary within 40 working days that the case has been forwarded, the financial intermediary is entitled to terminate the business relationship instead (Art. 9b GwG,

in force since 1 January 2023) — an exit right that keeps an inconclusive case from tying up the institution indefinitely, without requiring an artificial freeze in the meantime.

We ask that the same structure govern virtual-asset and stablecoin transactions: no continuous freeze merely because a report has been filed; a traceability requirement for significant transactions during MROS's analysis; a defined point at which the issuer may lift the measure if MROS has not responded — for an issuer the analogue is lifting the measure or redeeming against a traceable payout, since it cannot terminate a secondary-market holder it never onboarded; and, only once MROS actually forwards a case to a prosecution authority, a short, capped freeze pending that authority's decision. Section 7 sets out the specific figures we propose.

Step	GwG today — every financial intermediary	Proposal — stablecoin issuers
1	Suspicion arises at the intermediary that holds the customer file	Suspicion arises at the issuer, which has no customer relationship with the holder
2	Report to MROS (Art. 9)	**Freeze** — unilateral, executed on a public ledger
3	Client orders continue; paper trail preserved (Art. 9a)	Report to MROS
4	MROS forwards the matter to a prosecution authority and notifies the intermediary	Freeze held for 90 working days, if MROS confirms forwarding
5	**Vermögenssperre on MROS's notification — at most five working days** (Art. 10 para. 2); immediate only for authority-transmitted lists (Art. 10 para. 1bis)	Freeze held until the prosecution authority decides; absent a response, the issuer decides on its own risk assessment
Exit	Art. 9b — the intermediary may terminate if MROS is silent for 40 working days	None
Liability cover	Art. 11 GwG	None

Two points complete the picture. First, Swiss law already separates three cases. Sanctions designations — SECO and UN lists — freeze by operation of the embargo legislation and are reported to SECO, outside the GwG; the new duty to report should carve those out rather than duplicate them. Lists communicated under Art. 22a GwG trigger an immediate freeze and a report (Art. 9 para. 1 let. c, Art. 10 para. 1bis). Everything else is private suspicion, where the answer is report-and-analyse. The same three-way split should govern issuers: an immediate freeze in the first two cases; in all other cases a report first, with any freeze limited in time as it is for every other intermediary. Second, the party with less information about the

holder should not hold more power than the party with the customer file; if SIF intends to depart from the sequence adopted in 2016 for issuers, the explanatory report should say why the reasoning that led to it does not apply.

Two consequential points. A blacklisting is visible not only to the holder but to everyone, within minutes; the provision should state what the issuer may say to a holder who asks. And liability needs cover in both directions. Art. 11 GwG protects only breaches of secrecy and of contract; an issuer's relationship with a secondary-market holder is extra-contractual, so a good-faith freeze on a mistaken attribution needs an express exclusion of liability under Art. 41 OR. Conversely, an issuer that has reported but not frozen — as the sequence we propose contemplates — needs an express authorisation of the kind Art. 9a provides for intermediaries, since the Art. 8a capability duty would otherwise ground a Garantenstellung and Art. 305bis exposure for the omission. An overview of which actor can act against a stablecoin, on what legal basis and within what limits, is set out in the Annex.

The draft rightly conditions the notification on « soupçons fondés ». We ask that it be made explicit that a freeze applied on a sanctions-list match, at the request of an authority, or as a technical or precautionary measure does not of itself constitute such suspicion. Blur that line and the framework creates a perverse incentive: an issuer hesitates to freeze or block assets in situations of genuine uncertainty, precisely because doing so would look like an admission of suspicion. That outcome works against the AML/CFT objective, not for it.

We would also respectfully note a practical sequencing issue that may not be fully reflected in the current draft. In most real-world cases, an issuer will not itself be the first party to discover that a particular stablecoin address is connected to criminal conduct or should be frozen. More typically, that information will come from a third party (for example a victim, a blockchain-analytics provider, another financial intermediary or a foreign authority) and will be brought to law enforcement, which can then direct a freeze — by a seizure order under Art. 263 StPO or, where the information reaches MROS as a report, by a notification under Art. 10 GwG, a channel that today runs only to the intermediary that filed the report and that the draft does not yet extend to the issuer. The case in which the issuing financial intermediary obtains sufficient knowledge of the incident entirely on its own, and can therefore make the freeze-and-report decision without prior involvement of law enforcement, is likely to be the exception rather than the rule. We would therefore encourage the drafting to reflect this practical flow: outside the sanctions and Art. 22a cases described above, the issuer's duty to freeze should be triggered by an order from a Swiss authority — a seizure order or a notification from MROS — while information received from a third party gives rise, at most, to a duty to report under Art. 9 GwG, not to a duty to freeze. An issuer that executes such an order should be able to rely on it, with no liability toward the holder and an express right to lift the measure once the order lapses, rather than being expected to identify and assess the underlying incident independently.

7. 90-business-day period

The proposed 90-business-day freeze period is disproportionate when measured against the fiat baseline it should mirror. Under current law, a financial intermediary is never required to maintain a continuous freeze for anywhere near that long merely because a report is under MROS's review: orders continue to be executed during MROS's analysis (Art. 9a GwG), and even once MROS does forward a case, the resulting freeze is capped at five working days (Art. 10 para. 2 GwG). A 90-business-day continuous freeze for virtual-asset transactions would be a materially harsher regime than fiat institutions operate under today, and we see no basis in the nature of the assets themselves for that difference.

Our members' consistent view, following discussion within the association, is that crypto and stablecoin transactions should be governed by the same freeze/reporting architecture as fiat — not a separate, stricter one. Concretely, we ask for three elements, mirroring Art. 9a, 9b and 10 GwG:

- No continuous freeze while MROS conducts its own analysis of a report — mirroring Art. 9a GwG — subject to the same traceability requirement for significant transactions.
- A defined point at which the issuer may lift the measure if MROS has not responded, mirroring Art. 9b GwG: the same 40 working days already available for fiat, applied equally to virtual-asset and stablecoin transactions.
- Once MROS does forward a case to a prosecution authority, a freeze capped at five working days pending that authority's ruling — mirroring Art. 10 para. 2 GwG — rather than a freeze that can run for up to 90 business days.

MROS's own published statistics illustrate why 90 business days is excessive even against the existing 40-working-day fiat benchmark. In 2025, MROS received 21,087 suspicious activity reports and forwarded 1,375 of them to a prosecution authority — a ratio of about 6.5%, on our own calculation. Of the cases MROS forwarded between 2020 and 2023, MROS itself reports having had information on the further procedural outcome for only 35.7% of them as of 31 December 2024, rising to 49.7% as of 31 December 2025 — meaning that for roughly half of even the forwarded cases from that period, the outcome remained unknown five years on (MROS Annual Report 2025, Section 3.8). Against that backdrop, extending the existing 40-working-day standard to virtual-asset and stablecoin transactions is already a fair balance; the proposed 90-business-day period would more than double that wait without any corresponding gain in certainty, and MROS's own capacity constraints should not be passed on to financial intermediaries and their customers in the form of an even longer freeze.

Source: https://www.fedpol.admin.ch/dam/en/sd-web/05JKPvNkIrsY/jb-mros-2025-e.pdf (MROS Annual Report 2025)

This keeps the freeze proportionate at every stage: no open-ended freeze while MROS analyses a report, a defined exit point if MROS stays silent, and a short, capped freeze once MROS does act — applied identically to fiat and virtual-asset/stablecoin transactions. It also removes the incentive problem described in Section 6: because the issuer has a clear, bounded process throughout, a technical freeze is far less likely to calcify into a de facto indefinite one. In either design, the holder should be notified of the measure and its legal basis and have access to judicial review. Where MROS has not forwarded the case within the period, the issuer should have an express right to lift the measure and a good-faith safe harbour whichever way it decides — the draft's « propre évaluation des risques » gives the discretion without the cover. And since Art. 10 para. 2 counts « Werktage » while Art. 9b counts « Arbeitstage », SIF should say which the 90 « jours ouvrables » are.

Conclusion

If SIF takes up only three things from this letter, we would ask for these, in this order:

- The value threshold for Travel Rule identification and customer due-diligence should be raised to a level that makes a practical difference — CHF 5,000 or CHF 10,000 rather than CHF 500 (Section 3). At CHF 500 the exemption is barely used in practice, and a threshold set that low mainly displaces activity into fully unhosted, peer-to-peer transfers that regulators cannot see at all.

- The freeze/reporting mechanism for virtual-asset and stablecoin transactions should mirror the architecture that already governs fiat under Art. 9a, 9b and 10 GwG (Sections 6 and 7): no continuous freeze while MROS analyses a report, the same 40-working-day point at which the issuer may lift the measure if MROS stays silent, an immediate freeze only for sanctions designations and Art. 22a lists, and express liability cover both for a good-faith freeze and for not freezing after a report, and a freeze capped at five working days once MROS actually forwards a case to a prosecution authority — not a separate regime with a freeze that can run for up to 90 business days.
- The Travel Rule should be scoped to genuine payment orders between our customer and an identifiable external beneficiary — not to self-contained purchase, exchange or investment orders a customer places for their own account, including via DeFi (Sections 1 and 2) — paired with the realistic threshold in the first point above. The provision for transfers involving only one financial intermediary codifies the 2019 FINMA standard for third-party self-hosted wallets; it becomes usable only if the standard is to obtain information and establish control over the wallet rather than to identify a stranger as one would a client, and if the wording works in both directions.

Beyond these three, we also ask for further consideration of the extension of the transfer-information duty to fiat payments and its exemption mechanism (Section 1), of the scope and implementation of the stablecoin blacklist (Section 5) and of the customer due-diligence gap for virtual assets in standing business relationships (Section 4).

We understand your confidentiality request to pertain to the draft provisions you shared with us, rather than to SFA's own position on them.

We would be pleased to discuss these points further during our meeting on 24 September.

We remain at your disposal for any questions you may have.

Kind regards,

Michael Brüggler
President SFA

Florens Müller
Secretary SFA

Referenced legislation: Federal Act on Combating Money Laundering and Terrorist Financing (GwG, SR 955.0), in particular Art. 7a, 8a, 9a, 9b, 10 and 23 — https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/de; Anti-Money Laundering Ordinance (GwV, SR 955.01) — https://www.fedlex.admin.ch/eli/cc/2015/791/de; FINMA Anti-Money Laundering Ordinance (GwV-FINMA, SR 955.033.0), in particular Art. 11, 14, 20 and 51a — https://www.fedlex.admin.ch/eli/cc/2015/390/de.

Annex — Who can block a stablecoin, and on what legal basis

The table below sets out, for reference, which actor can act against a stablecoin at each point, on what legal basis, and within what limits. It underlies the sequence proposed in Sections 6 and 7.

Actor	Lever	Legal basis	Limits
Nobody — before execution	—	—	Every on-chain control is prospective and address-based; nothing operates before a transaction settles
Custodian / VASP — Swiss financial intermediary	Report to MROS (Art. 9); continued execution with the paper trail preserved (Art. 9a); an internal Softsperre — pre-execution review and delay — which is an operational measure, not a legal block; termination after 40 working days of MROS silence (Art. 9b)	Art. 9, 9a, 9b, 10, 10a GwG; Art. 11 protection	No freeze power of its own: the Art. 10 Vermögenssperre is executed only on MROS's notification — immediately only for authority-transmitted lists (Art. 10 para. 1bis) — and lasts at most five working days; may not inform the client, so even a delay cannot be explained (Art. 10a); reaches hosted wallets only
Issuer — token contract	Address-level freeze (e.g. the USDC blacklist function); for some tokens also destruction and re-issue (e.g. the USDT destroyBlackFunds function)	Contract code and issuer terms; no Swiss statutory basis or protection today	Prospective only; cannot identify the holder; cannot reach bridged or wrapped representations it did not deploy; freezing a pool, bridge or omnibus address immobilises every participant
Blockchain-analytics providers	Attribution of an address to an entity or a risk category	—	Probabilistic and cluster-level; not identification of a person
Bridge / layer-2 operator	Pause the bridge	—	Stops the flow, not the token
Nobody — immutable designs	—	—	Tokens on contracts with no administrative function (e.g. LUSD, RAI) cannot be frozen by anyone