finray

RESPONSE TO CONSULTATION PAPER CP26/13

Cryptoasset Perimeter Guidance

Observations on the proposed PERG 19 from the perspective of a regulated-finance technology vendor.

RESPONDENT	Finray Technologies Ltd
AUTHOR	Oleksandr Potapenko Founder & Chief Executive Officer
COMPANY NUMBER	HE 445903 (Cyprus Companies Registry)
SUBMITTED	14 May 2026
CONSULTATION	FCA CP26/13 — Cryptoasset Perimeter Guidance
CONSENT TO PUBLISH	Yes — name, role and company may appear in the FCA response register

SECTION 1

Respondent profile

LEGAL ENTITY	Finray Technologies Ltd
REGISTRATION	HE 445903 — Cyprus Companies Registry
REGISTERED OFFICE	Limassol, Republic of Cyprus
AUTHOR	Oleksandr Potapenko — Founder & Chief Executive Officer
ORCID ID	0009-0005-8936-1711
INFORMATION SECURITY	ISO/IEC 27001:2022 — certified December 2024 (NQA UK)
STRATEGIC PARTNERSHIP	TRM Labs Inc — Data Governance, Reseller and Mutual Referral arrangement, executed January 2026
CONTACT	partnership@finray.tech

Finray Technologies Ltd is a regulated-finance technology vendor. We build core banking, transaction monitoring and governance, risk and compliance (GRC) infrastructure for regulated financial institutions — banks, payment institutions, electronic money institutions and crypto-asset service providers ("CASPs") authorised under MiCA Articles 60 and 63.

Two facts are relevant to the credibility of the observations that follow.

ISO/IEC 27001:2022 certification. Finray's information security management system is certified to ISO/IEC 27001:2022 by NQA UK. The certificate covers the platform development and operations scope, including the cryptographic boundaries discussed in this response. The certificate is available under non-disclosure as part of vendor due diligence.

TRM Labs strategic partnership. Finray entered a Data Governance, Reseller and Mutual Referral arrangement with TRM Labs Inc in January 2026, publicly announced in February 2026. The partnership provides Finray's regulated-finance customers with on-chain analytics, sanctions screening and Travel Rule routing capability. Our observations on transaction-monitoring and Travel Rule architecture in this response are informed by the deployed reality of that partnership.

We respond to four of the six numbered consultation questions: Q2 (briefly), Q3, Q4 and Q5. We do not respond substantively to Q1 or Q6 — those questions invite comment on the introductory framing of PERG 19 and on consequential edits to PERG 1, 2 and 8, where our perspective does not differentiate from that of industry counsel.

SECTION 2

General observations

Three framings cut across our specific question responses.

The vendor lens

Finray operates infrastructure used by regulated firms; we do not act in any of the regulated cryptoasset activities ourselves. This perspective differs from that of an applicant CASP, an established authorised firm or a law firm ad-

vising on perimeter. Where the proposed guidance creates operational ambiguity, that ambiguity translates directly into procurement risk for our customers — and into design risk for the vendor population from which they procure. We comment on the proposed guidance from this position.

Cross-jurisdictional observation set

Finray maintains a forensic dataset of 53 MiCA CASP authorisations granted across 20 EU/EEA jurisdictions between January 2025 and April 2026, with companion analysis of deficiency patterns published at oleksandrpotapenko.com/mica-casp-licensing-forensic. Where useful, we reference observations from that dataset. The closest analogue in the proposed UK regime is also the largest single source of substantive comparative learning available to UK authorities: the Cryptoassets Regulations interact with — and partly diverge from — the MiCA perimeter in ways that affect cross-border firms.

The operational reality test

Throughout this response we apply a single test: under the proposed guidance, can a firm building, procuring or supervising the relevant infrastructure unambiguously identify what is and is not in perimeter? Where the proposed guidance leaves real-world business models in a grey zone, we say so and — where we can — propose a clarifying worked example.

QUESTION 2 OF 6

New specified investments

We agree with the proposed guidance set out in the New specified investments section. We offer two clarifying suggestions.

2.1 — Algorithmic stablecoin exclusion (§19.4.5)

We support the exclusion of algorithmic stablecoins from the definition of *qualifying stablecoin* on the basis that backing-asset holding is integral to the regulatory purpose. This is consistent with the MiCA Article 36 / Article 48 architecture, under which asset-referenced tokens and electronic money tokens are predicated on reserve assets and algorithmic mechanisms are not within scope of those activity categories.

We invite the FCA to consider an additional clarification: where a stablecoin product uses a hybrid reserve-and-stabilisation-mechanism design (for example, a partially collateralised stablecoin with a market-maker-driven peg), the threshold at which the design ceases to be a *qualifying stablecoin* is not addressed by §19.4.5 alone. A worked example would help applicants and supervisors apply the perimeter consistently.

2.2 — Three-limb issuance test (§19.5.1)

The three-limb test (offer + redemption + reserve holding from a UK establishment) is operationally clear at the conceptual level. We invite one clarification: where the offer limb is delegated to a third-party platform operating under article 9M(4)(c) outsourcing arrangements, but the redemption and reserve-holding limbs remain with the issuer, §19.5.5 confirms that the issuer remains the issuer. However, the territorial analysis under §19.3.4 (deeming provisions of section 418(6B)) becomes complex where the outsourced platform is overseas. We recommend the FCA add a worked example covering a UK-issued qualifying stablecoin where offer is delegated to a non-UK distribution platform, to clarify the perimeter outcome for the platform itself.

QUESTION 3 OF 6

New regulated cryptoasset activities

We agree with the structural position taken in this section. We comment substantively on three areas where the proposed guidance creates operational ambiguity for vendors and firms building the infrastructure, or where it diverges from comparable jurisdictions in ways that affect cross-border firms.

3.1 — Non-application of the Overseas Persons Exclusion (§19.3.5)

We support the proposed §19.3.5 confirmation that the Overseas Persons Exclusion ("OPE") at PERG 2.9.17G does not apply to regulated cryptoasset activities. Section 418(6C) is the appropriate territorial trigger.

We note that this is a structural divergence from the MiCA Article 61 third-country reverse-solicitation regime. Under MiCA Article 61, a third-country firm is permitted to provide a crypto-asset service to an EEA client at the client's own exclusive initiative, without MiCA authorisation, provided the firm does not solicit. The UK perimeter, in contrast, captures any overseas firm involved in the sale or subscription of a *qualifying cryptoasset* to or by a UK consumer, unless an authorised intermediary is interposed between the overseas firm and the consumer (per §19.3.1(4)).

The practical consequence is that a MiCA-authorised CASP — for example, one of the 12 CASPs authorised in Germany or the 11 authorised in the Netherlands as at April 2026 — that currently provides services to UK retail residents on a reverse-solicitation basis will require dual authorisation. This is, in our observation, a perimeter outcome that has not yet been internalised by the majority of MiCA-authorised CASPs, several of which were granted authorisation on the basis of a target market that explicitly included UK clients under what was assumed to be a similar reverse-solicitation framework.

We do not propose a change to the substantive position. We do recommend the FCA add a worked example along the following lines, to assist applicants in self-assessing perimeter outcomes:

> SUGGESTED WORKED EXAMPLE — §19.3.5
>
> Firm A is authorised under MiCA Article 60 in an EEA Member State to provide custody and trading services in crypto-assets. A maintains a website that is accessible to UK residents but does not target UK consumers; UK consumers find the website by their own search. Some UK consumers subscribe to A's services and execute trades on A's platform. A has no authorised UK intermediary interposed between A and the UK consumer. Under section 418(6C) of the Act, A is deemed to be carrying on regulated cryptoasset activities in the UK, notwithstanding the absence of solicitation. A requires Part 4A authorisation.

3.2 — Safeguarding territorial test and MPC / threshold signature architectures (§19.3.2, §19.6.2)

§19.3.2 establishes that the place of supply for safeguarding cryptoassets is the location of the safeguarding operations — specifically, where the requisite degree of control to bring about a transfer is exercised. §19.6.2 confirms that the requisite degree of control includes arrangements where the firm engages other persons to hold "shards" of a private cryptographic key.

We welcome both points. The architectural acknowledgement of key-shard arrangements is appropriate and reflects the operational reality of how regulated crypto-asset custody is built in practice. However, the territorial application creates an unresolved question for threshold-signature arrangements — including the multi-party computation ("MPC") protocols that constitute the dominant institutional-grade custody design in 2026.

In a typical 2-of-3 or 3-of-5 threshold signature scheme:

- Each shard is held in a separate jurisdiction (commonly: one in the operational jurisdiction of the firm, one in a counterparty-controlled jurisdiction, one in a fully geographically separate jurisdiction for disaster recovery);
- No single shard is sufficient to authorise a transfer;
- A signature is reconstituted via a cryptographic protocol that does not at any point assemble a complete private key in cleartext;
- The "orchestrator" — the firm operating the signing protocol — may be in a fourth jurisdiction.

Under the §19.3.2 test, the determination of "place of safeguarding operations" depends on whether the FCA looks to (a) the location of any shard, (b) the location of the orchestrator, (c) the location where the protocol's signature output is broadcast to the relevant blockchain, or (d) some weighted combination. The current draft of §19.3.2 does not address this question, and §19.6.2 — while acknowledging shard arrangements as in-scope of safeguarding — does not address territoriality.

The practical consequence is that the territorial perimeter of safeguarding becomes indeterminate for a substantial portion of the institutional custody market, which today is built on threshold MPC.

We invite the FCA to clarify the territorial test for MPC and threshold-signature arrangements. A worked example along the following lines would assist:

> SUGGESTED WORKED EXAMPLE — §19.3.2
>
> Firm B operates a custody platform on behalf of UK consumers using a 2-of-3 threshold signature scheme. Shard 1 is held by Firm B in the United Kingdom. Shard 2 is held by an unrelated infrastructure provider in Singapore. Shard 3 is held by Firm B in a geographically separate disaster recovery site in Estonia. Firm B's signing orchestrator software runs in the United Kingdom. The FCA considers that Firm B is safeguarding cryptoassets in the United Kingdom because the orchestrator — the locus of control over the signing process — is established in the United Kingdom, notwithstanding that two of the three shards are extraterritorial. Firm B's authorisation does not extend to and is not required of the Singapore or Estonian shard holders, provided those holders are not themselves authorised, and the arrangements are described in the firm's CASS reports.

This is not a hypothetical scenario. It is the default institutional architecture in 2026.

3.3 — QCATP interfaces and the "person operating the platform" test (§19.7.1, §19.7.5)

§19.7.1 sets out four cumulative elements of a QCATP: a trading system, multiple third-party buying and selling interests interacting within the system, an arrangement that results in a contract, and the contract being for the exchange of qualifying cryptoassets for money or other qualifying cryptoassets.

§19.7.5 sets out the position on interfaces connecting users to automated protocols, including the observation that perimeter inclusion depends on whether the regulated activity is carried on by way of business by an identifiable person, and that perimeter assessment is fact-specific.

We invite the FCA to consider that "an identifiable person" is the load-bearing concept and that, in the context of decentralised exchange ("DEX") frontend interfaces and aggregator services, this test is not well-developed in the current draft. There is a substantial population of operators who:

- Develop and maintain a frontend web interface that allows users to specify trade parameters;
- Submit transactions to one or more automated smart-contract protocols that perform the trade;

- Do not custody assets at any point in the flow;
- May or may not earn fees from the trade;
- May or may not run order-flow optimisation logic ("aggregators").

Some of these operators clearly fall within *arranging deals in qualifying cryptoassets* per §19.8. Others — for example, a pure software project publishing open-source frontend code — clearly do not. The intermediate cases (a frontend operator who runs aggregator routing across multiple automated protocols and earns a fee on each trade) are where the perimeter is least clear.

We recommend the FCA expand §19.7.5 with one worked example each of: (a) a clearly in-perimeter aggregator-style frontend; (b) a clearly out-of-perimeter pure-publication frontend; and (c) the intermediate case that operators are most likely to face in practice — where the perimeter assessment will turn on specific facts.

QUESTION 4 OF 6

Exclusions relevant to the activities

We agree with the proposed exclusions. We comment on four exclusions where the proposed guidance creates real-world operational questions.

4.1 — Self-custody and the negative-control distinction (§19.6.3)

§19.6.3 makes the foundational distinction: where a firm supplies a customer with a solution for the customer to keep their own cryptoasset secure by exercising control themselves, and the firm has no means to bring about transfer, the firm is not safeguarding. Where the firm contractually undertakes not to exercise control but actually retains the capability — for example, an override mechanism — the control element is likely met.

We welcome this distinction. It is correct and architecturally precise. However, the practical application to commonly deployed infrastructure-vendor patterns is unclear in three specific cases.

(a) Emergency recovery rights

Customer-key-management infrastructure is, in practice, almost always delivered with vendor-side emergency recovery capability — typically a sealed-key escrow scheme, a court-order-triggered recovery, or a vendor-administered social recovery quorum. The vendor's contractual commitment is not to invoke these rights absent specified conditions. Under the proposed §19.6.3 reading, does the existence of such a capability — coupled with a contractual non-exercise undertaking — constitute "requisite degree of control"?

(b) Firmware update access

Hardware Security Module ("HSM") and secure enclave infrastructure ships with firmware-update capability that necessarily includes the ability to modify the cryptographic boundary. The vendor's contractual undertaking is not to use firmware update to extract or substitute keys, but the technical capability remains. Does the firmware-update channel create "requisite degree of control"?

(c) Compliance-driven key rotation

UK regulators may, in extremis, require a firm to rotate cryptographic keys for an entire customer base. Vendors of customer-key-management infrastructure typically retain the operational capability to execute such rotation on the firm's instruction. Does this constitute control by the vendor, by the firm, or by neither?

The current §19.6.3 draft places a substantial population of bona-fide infrastructure vendors in an uncertain perimeter position. The vendor population in question includes the institutional-grade HSM vendors selling to UK CASPs, the secure-enclave-based key-management vendors, and the MPC vendors discussed in Section 3.2 above.

We recommend the FCA clarify §19.6.3 with one or more worked examples covering vendor-retained capabilities that are contractually constrained, including specifically the emergency-recovery, firmware-update and compliance-rotation scenarios above. The clarification need not change the substantive position — it should make explicit what is currently implicit.

4.2 — Holding-out exclusion (§19.6.9)

§19.6.9 sets out the article 9R(2) holding-out exclusion: a person who has the requisite degree of control but does not hold themselves out as providing a safeguarding service falls outside the regulated activity.

The §19.6.9 worked example — a safety deposit box provider or generic data storage provider with incidental control over keys stored by customers — is a good illustration but a narrow one. We observe that the same exclusion is highly relevant to two other categories of infrastructure.

(a) Generic cloud storage and document management

Where a UK CASP stores its private-key shards (or backups) in a generic enterprise cloud storage product, the cloud provider has the technical capability to access the stored data. The cloud provider does not hold itself out as a cryptoasset safeguarding service. Under §19.6.9, the cloud provider is outside the perimeter. We welcome this implication and invite the FCA to confirm it explicitly, as the alternative reading would bring substantial parts of the UK cloud-infrastructure industry within scope.

(b) Database and infrastructure-as-a-service vendors

Similar logic applies to database providers, container-orchestration platforms and infrastructure-as-a-service vendors whose customers happen to be CASPs storing key material on the vendor's infrastructure.

The clarification matters because, in our experience, the procurement teams of UK CASP applicants frequently raise the question with their vendor counterparties as part of due diligence. A clarifying paragraph in §19.6.9 would short-circuit a substantial volume of vendor due diligence correspondence that is currently occurring without an authoritative reference.

4.3 — Temporary settlement exclusion (§19.6.6)

§19.6.6 introduces an exclusion for safeguarding carried out temporarily to facilitate the settlement of a transaction, with the FCA's preliminary view that "temporarily" is unlikely to require longer than 24 hours from the point at which the requisite degree of control exists.

We support the principle and the 24-hour anchor. However, the modern settlement reality for institutional cryptoasset trading includes:

- **T+0 settlement on QCATPs.** Most UK QCATP applicants will operate intra-day settlement.
- **T+1 or T+2 settlement with overnight float.** Cross-border settlement between an overseas trading venue and a UK custodian may produce a 24—48 hour window between trade execution and final settlement.
- **Block-trade settlement.** Institutional block trades may require additional time for matched-principal execution, position confirmation and on-chain final settlement.

We invite the FCA to consider expanding the 24-hour preliminary view to explicitly accommodate the institutional-settlement use cases, perhaps via a worked example along the following lines:

> SUGGESTED WORKED EXAMPLE — §19.6.6
>
> Firm C operates a UK QCATP. Trades execute on the platform with notional settlement T+1. Firm C uses a single operational wallet to receive cryptoassets in for settlement and to pay cryptoassets out following matched settlement. The cryptoassets are in Firm C's control for, on average, 28 hours from trade execution to final settlement. The FCA considers that this duration is consistent with "temporary" for the purposes of article 9Q, provided Firm C does not use the settlement wallet for any purpose other than facilitating the settlement of trades on the QCATP.

4.4 — Group company exclusion (§19.6.5)

§19.6.5 sets out the article 9O group company exclusion: safeguarding carried on by a bare nominee on behalf of a customer of an authorised group entity is excluded from the safeguarding activity, provided the authorised entity has accepted responsibility.

We support the exclusion. We invite the FCA to clarify one operational question: where the bare nominee is incorporated in a jurisdiction other than the UK (for example, an offshore subsidiary of a UK-authorised parent), does the exclusion still apply? The drafting of article 9O is neutral as to the location of the nominee, but §19.6.5 is not explicit. A clarification would assist UK-authorised groups that operate offshore custodial subsidiaries for legitimate tax-structuring or regulatory-arbitrage-mitigation reasons.

QUESTION 5 OF 6

Interaction with MLR framework

We agree with the structural position. We comment substantively on three points where the proposed guidance, in our submission, understates the operational lift involved or leaves operational questions unresolved.

Our observations on this section are made from the operational position of a vendor whose Travel Rule and transaction-monitoring infrastructure is deployed today under the FCA's MLR cryptoasset register supervisory regime, in partnership with TRM Labs Inc (Data Governance, Reseller and Mutual Referral arrangement entered into in January 2026, publicly announced in February 2026).

5.1 — The MLR-to-FSMA operational gap

A firm currently registered with the FCA as a Cryptoasset Exchange Provider under MLR has, in our observation, typically built the following infrastructure stack:

- Transaction monitoring aligned to JMLSG Part III Chapter 23 (cryptoasset) and the FCA's SUP 17A reporting framework, with rule sets calibrated to AML/CTF risk;
- Travel Rule routing under regulations 64A to 64H of the Money Laundering Regulations 2017 (as amended by SI 2022/860) and the FCA's published expectations for cryptoasset businesses complying with the UK Travel Rule, with counterparty look-up infrastructure typically built on TRM Labs, Notabene or Sumsub partnerships;
- Sanctions screening against UK OFSI, EU and OFAC consolidated lists;
- Customer due diligence and ongoing monitoring aligned to MLR Part 3.

That stack is fit for the MLR perimeter — an AML/CTF supervisory regime. The FSMA Part 4A perimeter additionally requires:

- **Market integrity surveillance** — including market-abuse monitoring, manipulation detection and best-execution monitoring under COBS 11, none of which is required under MLR;
- **Conduct of business compliance** — including suitability, appropriateness, communications, and product governance under COBS, where applicable to the relevant cryptoasset activity;
- **Client asset compliance under CASS** — including the safeguarding obligations under article 9N, evidenced via daily reconciliation and external auditor attestation;
- **Senior Manager and Certification Regime ("SMCR") accountability** — including SMF prescribed responsibilities for safeguarding and operational resilience;
- **Operational resilience** — under SYSC 15A, including important business service identification, impact tolerance setting and self-assessment.

These are not extensions of the MLR-era stack. They are substantively new surfaces, requiring new tooling, new policies, new controls and new evidence-collection workflows. Our observation across both the MLR-registered UK cohort and the MiCA-authorised EEA cohort is that the transition timeline implied by §19.1.12 — under which a firm must apply for Part 4A authorisation and notify the FCA within 30 days of regime commencement — is plausible only for the largest firms with substantial existing investment in non-MLR compliance infrastructure.

We recommend the FCA publish, in advance of or alongside the final Policy Statement, a transition map for MLR-registered firms covering:

1. **MLR-era monitoring obligations** that must remain operative during the FSMA transition window — to avoid a gap during the registration-to-authorisation handover;
2. **FSMA-era systems and controls** that must be operative at Part 4A authorisation grant — broken down by activity (article 9M, 9N, 9S, 9T, 9W, 9Y, 9Z6);
3. **Sequencing of CASS and COBS applicability** relative to permission go-live — specifically, whether obligations under CASS 6 (or its cryptoasset equivalent) attach at authorisation grant or on a transitional schedule;
4. **SMCR accountability mapping** — confirmation that, for cryptoasset-only firms, the SMF responsibilities for safeguarding, transaction monitoring and operational resilience are clearly allocable.

This is, in our experience, the area in which firms most commonly underestimate the implementation curve. In the MiCA authorisation forensic dataset at oleksandrpotapenko.com/mica-casp-licensing-forensic, the operational-controls build (covering analogous CASS, COBS and operational resilience equivalents under MiCA Title V and DORA) was a frequent rate-limiting workstream in the authorisation timeline. The UK position will not, in our view, be materially different.

5.2 — Annex 1 Financial Institutions and the dual-status prohibition

§19.1.12 confirms that a firm cannot be both an Annex 1 Financial Institution under MLR and an authorised person under Part 4A. We support the clarity of this position.

We invite the FCA to confirm one corollary: where a firm currently registered as an Annex 1 FI carries on multiple business lines, only one of which is in scope of the new regulated cryptoasset activities, the firm has the option of separating the cryptoasset business into an authorised subsidiary while retaining Annex 1 FI status for the remaining business. The drafting of Regulation 55(2) MLR does not appear to preclude this structure, but the position is not explicit in §19.1.12.

5.3 — Travel Rule alignment

The Travel Rule regime under the Money Laundering Regulations cryptoasset provisions, FATF Recommendation 16 and the corresponding EU Transfer of Funds Regulation (Regulation (EU) 2023/1113) is operative today across the UK and EEA cohort. We invite the FCA to confirm that the FSMA Part 4A regime does not introduce additional Travel Rule obligations distinct from those in the MLR regime. The current §19.12 drafting does not contradict this, but firms preparing their transition plans require explicit confirmation that they are operating under a single Travel Rule regime, supervised under MLR, with Part 4A authorisation providing the prudential and conduct envelope around it.

For further observations on the operational architecture of the Travel Rule, see commentary at finextra.com/blogposting/31644.

CLOSING

Summary and cross-references

We are grateful for the opportunity to comment on CP26/13. We do not respond to Question 1 (introduction to PERG 19) or Question 6 (consequential edits to PERG 1, 2 and 8), where our perspective does not differentiate from that of industry counsel.

We would be pleased to engage further with the FCA at the policy-statement drafting stage, on any of the points raised above and in particular on the MPC / threshold-signature territoriality clarification at Question 3.2 and the MLR-to-FSMA transition map at Question 5.1.

Cross-references cited in this response

MiCA CASP licensing forensic dataset
53 authorisations across 20 EU/EEA jurisdictions, deficiency-pattern analysis.
oleksandrpotapenko.com/mica-casp-licensing-forensic

MiCA Survival Guide
Comprehensive 8-section guide to MiCA licensing for crypto-asset service providers.
oleksandrpotapenko.com/mica-survival-guide

DORA compliance challenge
Technical gauntlet for cryptoasset firms under DORA — transferable observations to UK SYSC 15A.
oleksandrpotapenko.com/dora-challenge

Travel Rule is not a compliance bolt-on — it is an identity routing problem
Finextra commentary on the operational architecture of the Travel Rule.
finextra.com/blogposting/31644

Safeguarding account reconciliation is not a reporting function — it is a solvency discipline
Finextra commentary on safeguarding architecture.
finextra.com/blogposting/31643

Finray Technologies corporate site
Platform documentation, partnerships, and Intelligence radars.
finray.tech

Oleksandr Potapenko
Founder & Chief Executive Officer
Finray Technologies Ltd — HE 445903, Limassol, Cyprus
partnership@finray.tech • ORCID 0009-0005-8936-1711