FORENSIO · CONCEPT PAPER · JULY 2026 ROADMAP CONCEPT — NOT YET A SHIPPING FEATURE

Collaborative AML Without Data Pooling

Forensio Beacon: pseudonymised risk signals exchanged directly between banks' on-premise instances — no central platform, no raw data egress, every exchange sealed in both audit trails.

1 · The gap criminals live in

Criminal networks operate *across* institutions; each bank investigates *inside* its own walls. Collaborative monitoring demonstrably closes that gap: in Estonia, ten banks running a shared intelligence channel resolved 1,400+ joint investigations in nine months, prevented roughly €3M from reaching criminal accounts, and cut typical case coordination from days to minutes. Singapore's COSMIC platform put legal-person misuse, trade-finance abuse and proliferation financing on a statutory sharing footing.

But every implementation to date shares one architecture: **a central platform that sees the data.** Centralised pooling is legally fragile (the Dutch TMNL consortium had to cut back scope under data-protection pressure), it concentrates breach risk in one honeypot, and it is structurally unusable by institutions whose first requirement is *data never leaves* — which increasingly describes the sovereignty-conscious European market.

> *The question is not whether banks should share risk intelligence — regulators on both sides of the Atlantic now actively encourage it. The question is whether sharing requires surrendering data to a third party. It does not.*

2 · How a Beacon exchange works

- **Entity fingerprints.** Each bank's on-prem instance derives salted, keyed hashes of case entities (normalised names, strong identifiers). Salts are partnership-scoped: fingerprints are comparable inside the partnership and meaningless outside it.
- **Minimal query, minimal answer.** "Has any partner sealed a decision involving this fingerprint?" The response is *yes/no*, a coarse risk class, and a compliance-to-compliance contact point. Never case detail, never amounts, never customer data — and **never whether a report was filed** (that would be tipping-off, and it is excluded from the signal set by design).
- **Both sides seal the exchange.** The query and the response each become tamper-evident events in *both* banks' hash-chained ledgers. Collaborative AML where the sharing itself is a first-class audit artifact — reviewable by each bank's supervisor without any central operator.
- **Responses are context, not cargo.** A Beacon answer enters the receiving investigation as one more piece of classified evidence; it cannot be exported or forwarded. Onward-sharing restrictions are enforced by construction, not by policy memo.

3 · A legal home on both sides of the Atlantic

Regime	Basis	What the Beacon kit ships
EU	AMLR Art. 75 information-sharing partnerships — with pseudonymisation *mandated*, a data-protection impact assessment and supervisor notification before start	partnership DPIA template · supervisor-notification pack · joint-controllership skeleton · the pseudonymisation design (the fingerprint scheme is the mandated pseudonymisation)
EU, before the partnership	the long-standing exception permitting two institutions on the *same customer, same transaction* to compare notes	point-to-point mode — the lowest-risk starting configuration
US	PATRIOT Act §314(b): a statutory safe harbor for voluntary inter-institution sharing; the method is explicitly open, and 2026 FinCEN guidance expanded the scope to fraud and encourages participation	314(b) registration workflow · security & confidentiality procedures · the same protocol, a different rulebook

Filing never touches Beacon: reports go to FIUs through the normal channel. Beacon carries investigation context only, beneath the tipping-off line.

4 · Why only an on-prem architecture can build this

- **Zero egress and collaboration stop being a trade-off.** Signals travel; data does not. Air-gapped institutions can participate through a controlled diode/batch pattern — impossible with any central-platform design.
- **No operator to breach, subpoena or outgrow.** There is no third party holding the pooled book of every member's suspicions.
- **Audit falls out of the architecture.** Forensio decisions already seal into hash-chained records; Beacon events reuse the same discipline. For platform vendors this would be a new trust subsystem; here it is a by-product.
- **Network effects favour the earliest members.** Every additional institution makes each member's signals more valuable — the design-partner cohort becomes the founding partnership.

5 · Status and the path to live

Beacon is a **roadmap concept**: the protocol specification and the counsel review of the signal taxonomy come first; the reference implementation — two Forensio instances exchanging sealed signals on one demonstration machine — follows; a live partnership launches with pilot institutions under the EU or US wrapper. Institutions interested in shaping the founding partnership can reach the team at hello@forensio.com.

Forensio — policy-bound, on-prem AI decisioning for financial crime. AI agents investigate; a deterministic engine certifies what is permissible; a human decides; every decision seals into a hash-chained record. forensio.com · hello@forensio.com. This concept paper describes a roadmap capability and summarises legal positions at concept level; it is not legal advice and no capability described here is represented as currently shipping.