

# FALCON Tools for the Financial Sector

## Distinctive Value for AML, Sanctions and Fraud Compliance

FALCON | Horizon Europe Grant Agreement No. 101121281

---

FALCON develops data-driven tools to fight large-scale corruption and organised crime. Several of these tools are of direct value to banks for anti-money laundering, sanctions and fraud compliance. This note sets out what they offer, where they are distinctive, how mature they are, and how a financial institution can engage with them.

### What FALCON offers

**The knowledge base is the backbone.** At the core of FALCON is a domain model and the knowledge base built on it, which fuses heterogeneous sources, corporate and beneficial-ownership data, PEP records, procurement, financial transactions, crypto and open-source information, into a single queryable model. It represents persons, public and corporate organisations, ownership structures, events and the relations between them: the same substrate that underpins money laundering, sanctions circumvention and fraud. It is specialised for corruption through its indicator layer and, by design, it also models the interlinks with other forms of crime. The analytical tools do not sit side by side: they populate this layer and reason over it. The result is one investigative picture rather than a set of point tools, turning data that institutions often already hold into connected, usable insight.

**Explainable by design, aligned with the EU AI Act.** The corruption risk assessment (ACRA) and the trustworthy, white-box AI components are built for transparency from the outset, with explainable outputs, for example through SHAP and LIME. Depending on their intended purpose, AI systems used in these contexts may fall within the high-risk regime of the EU AI Act (Article 6(2) in conjunction with Annex III); explainability, human oversight and documentation are in any case central supervisory expectations, which this design choice directly supports. An AP4AI assessment has been conducted for ACRA. Explainability is a built-in principle, not an added module.

**Network reasoning over the knowledge base.** Because the data is held in a semantic model, the investigation and decision-support tools (RAIDS) and the hidden-pattern analysis can apply graph and probabilistic reasoning across sources: revealing ultimate beneficial owners, indirect links to sanctioned entities or PEPs, and multi-hop layering chains. FALCON orients this specifically to the opaque corporate structures and criminal networks behind sanctions circumvention, such as tracing assets concealed through transnational corporate schemes.

**Crypto and fiat in one environment.** The crypto-asset analysis component (Kriptosare) feeds the same model, supporting the growing need to cover the crypto-fiat crossover within a single environment and to apply to digital assets the same rigour used for fiat transactions.

**A corruption and sanctions lens that complements AML.** FALCON is purpose-built for large-scale corruption and organised crime, with corruption indicators, procurement analytics and risk assessment. As corruption is a primary predicate offence for money laundering, this lens complements banks' AML systems on exactly the predicate-offence and sanctions-circumvention side that generic transaction monitoring tends to cover less, while resting on an entity and relationship model that is common to financial crime as a whole.

**Distinctive combination.** The distinctiveness of FALCON lies in the combination and the focus, not in the sole possession of any single technique. Semantic models and graph

analytics are mature technologies; what is distinctive is the domain model that organises them, the fusion of sources that are hard to combine, explainability aligned with the EU AI Act, and coverage from procurement to crypto, in an EU-funded, interoperable solution validated with law enforcement. FALCON is positioned not as another transaction monitor, but as a complementary investigative capability that improves the efficiency and effectiveness of compliance.

## What this means in practice

The tools are validated prototypes, not finished off-the-shelf products. The table sets out what each does for a bank and how mature it is.

| Component                                                 | What a bank can do with it                                                                                                                                                         | Maturity                                          |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Knowledge base and data layer (CRM, DAA toolkit)          | Bring corporate and beneficial-ownership data, PEP records, procurement, transactions, crypto and open-source information into one queryable picture of a counterparty or network. | TRL 6, target 7. Validated in the project pilots. |
| Investigation and hidden-pattern tools, dashboard (RAIDS) | Work an alert as a network, not transaction by transaction: surface indirect links to sanctioned entities or PEPs, multi-hop layering chains and relations hidden across sources.  | TRL 6, target 7.                                  |
| Corruption risk assessment (ACRA)                         | Score counterparty and procurement-linked corruption risk, with explainable outputs that can be shown to an auditor or supervisor.                                                 | TRL 7.                                            |
| Crypto-asset analysis (Kriptosare)                        | Trace crypto exposure and the crypto to fiat crossover in the same environment as traditional data.                                                                                | Validated prototype, TRL 6 to 7.                  |
| Trustworthy AI components                                 | Apply white-box models and controls supporting the oversight, documentation and explainability expected of high-risk AI systems.                                                   | TRL 4, target TRL 6.                              |

Table 4. FALCON tools relevant to the financial sector.

## Access and licensing

**Fair and reasonable conditions.** Access to the results is granted on fair and reasonable terms, which under the EU framework may include financial terms or royalty-free conditions, depending on the circumstances.

**Software, not source code.** The tools are provided in object code, as container images and through wrapper APIs. They can be cloud-hosted and sit alongside existing systems. Source code is not provided.

**Data is licensed separately.** The heaviest restrictions fall on data, not on the tools: third-party commercial sources are licensed separately, and some contributed data carries non-commercial conditions.

**Public authorities.** EU institutions and national authorities receive royalty-free access for non-commercial policy and operational use. Private-sector engagement follows the separate route below.

## How a financial institution can engage

At this maturity, the primary route for the private sector is a co-development and validation partnership, not an off-the-shelf purchase.

- The institution contributes real operational data, domain expertise, a validation environment and resources.
- It gains early access, influence over the roadmap, and an implementation hardened and customised for its own use cases.
- Intellectual property is settled up front: background stays with its owners, and results of the co-development are governed by the partnership agreement.
- Commercial licensing, SaaS and services remain available as tools mature beyond TRL 7.

Engagement with the sector runs through validation and co-development partnerships and through the discussion within the European banking sector.

---

FALCON has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101121281. The views expressed are those of the consortium and do not necessarily reflect those of the European Union.