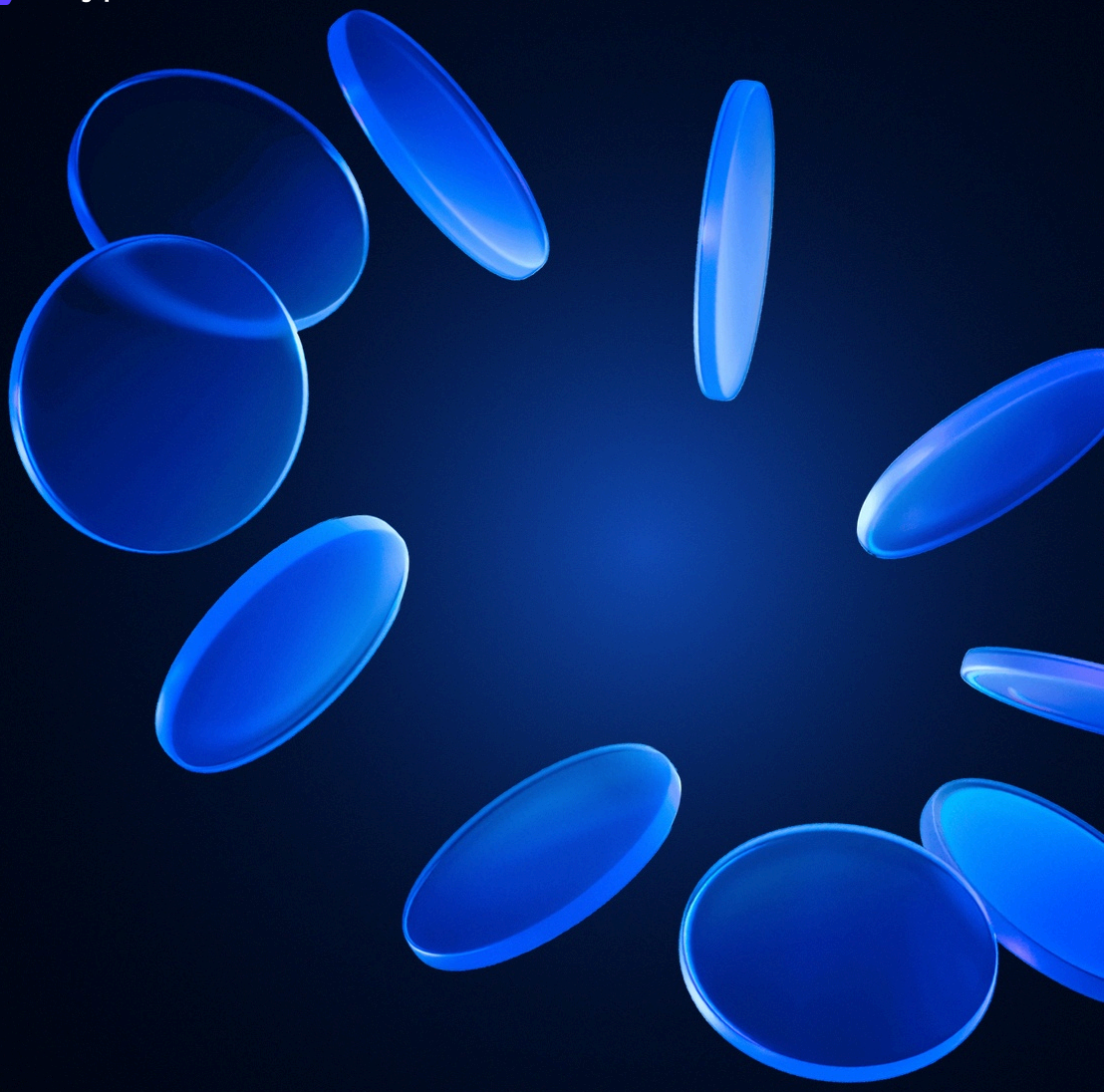
JOINT WHITEPAPER · 2026

Lukka | CryptoSwift



From Risk Score to Release Decision

How blockchain analytics and the Travel Rule work together

PUBLISHED
November 16, 2026

AUTHORS
Lukka · CryptoSwift

TOPICS
Blockchain analytics · Travel Rule · AML

INSIDE THIS PAPER

Contents

00 Two questions behind every transfer 3

INTRODUCTION

01 What makes a blockchain analytics methodology defensible 4

SECTION 1 | METHODOLOGY

02 Turning the risk score into a transaction decision 10

SECTION 2 | DECISIONING

03 Processing stablecoins: what changes 12

SECTION 3 | STABLECOINS

04 The score is where the decision begins 13

CONCLUSION

Lukka

Founded in 2014, Lukka provides enterprise blockchain data and software solutions to financial institutions, exchanges, fund administrators and government agencies. Its platform transforms raw on- and off-chain activity into audit-ready intelligence for accounting, compliance, risk and reporting.

CryptoSwift

CryptoSwift connects Travel Rule compliance with blockchain analytics, AML sanctions screening and Enhanced Due Diligence, so every transfer is screened, decided and documented before funds move.

INTRODUCTION

Two questions behind every transfer

Blockchain analytics tells a VASP how risky a wallet and its funds are. The Travel Rule tells it who is on the other side of a transfer. This paper explains how blockchain risk is measured, how that measurement drives decisions alongside Travel Rule workflows, and why the two are strongest operating as joint controls, powered by Lukka and CryptoSwift.

Every crypto-asset transfer a VASP or bank processes raises two questions: *is the money risky*, and *who is behind it?* Neither discipline answers both on its own.

Blockchain analytics sees addresses, flows and the entities that control them. But for a wallet, the blockchain shows the wallet's history and risk level, potentially accompanied by the custodian's risk level, not the identity of the customer behind a given transaction. Travel Rule messaging fills that gap by exchanging originator and beneficiary information between VASPs. Similarly, regulation requires custodians to collect or even verify the identity information underlying transactions with self-hosted wallets. The Travel Rule data focuses on identities, but says nothing about where the funds have been.

That gap has never mattered more. MiCA is now fully in force following the end of its transitional period on 1 July 2026. The Transfer of Funds Regulation, which defines Travel Rule obligations in the EU, has applied to crypto-asset transfers since December 2024, and the AML Regulation arrives in July 2027, placing crypto-asset service providers under the same due diligence framework as banks. This means that in addition to Travel Rule and on-chain risk assessment operations, digital currency payments are also subject to AML sanctions and watchlist screening as well as Enhanced Due Diligence requirements. Regulators expect institutions to have 360-degree visibility into each transaction, and to show how they reached every compliance decision. The common thread is the risk-based approach: controls calibrated to an institution's own risk, with each outcome explainable to an examiner.

This paper follows a transfer from screening to decision across Lukka's blockchain analytics and CryptoSwift's Travel Rule tooling: the methodology that produces a defensible blockchain risk score, how a rule engine turns that score into a release decision before funds move, how to handle the mandatory Travel Rule operations, and what changes when the asset being moved is a stablecoin.

SECTION 1

What makes a blockchain analytics methodology defensible

A risk score is only as good as the methodology behind it, yet there is no industry standard for how blockchain risk is measured. Each provider defines its own categories, weights, labels and scoring logic, so two providers can screen the same wallet on the same day and reach different conclusions.

For an institution, that difference is not academic. When a score blocks a withdrawal, clears an onboarding or supports a suspicious activity report, the institution, not the vendor, must defend it. The question is not which provider returns the highest or lowest score. It is whose score can be explained, evidenced and aligned with the institution's own risk assessment.

Six dimensions separate a defensible methodology from a weak one. On each, there is a common shortcut, and there is the approach built into Lukka Blockchain Analytics.

EXHIBIT 1 | SIX DIMENSIONS OF A DEFENSIBLE METHODOLOGY

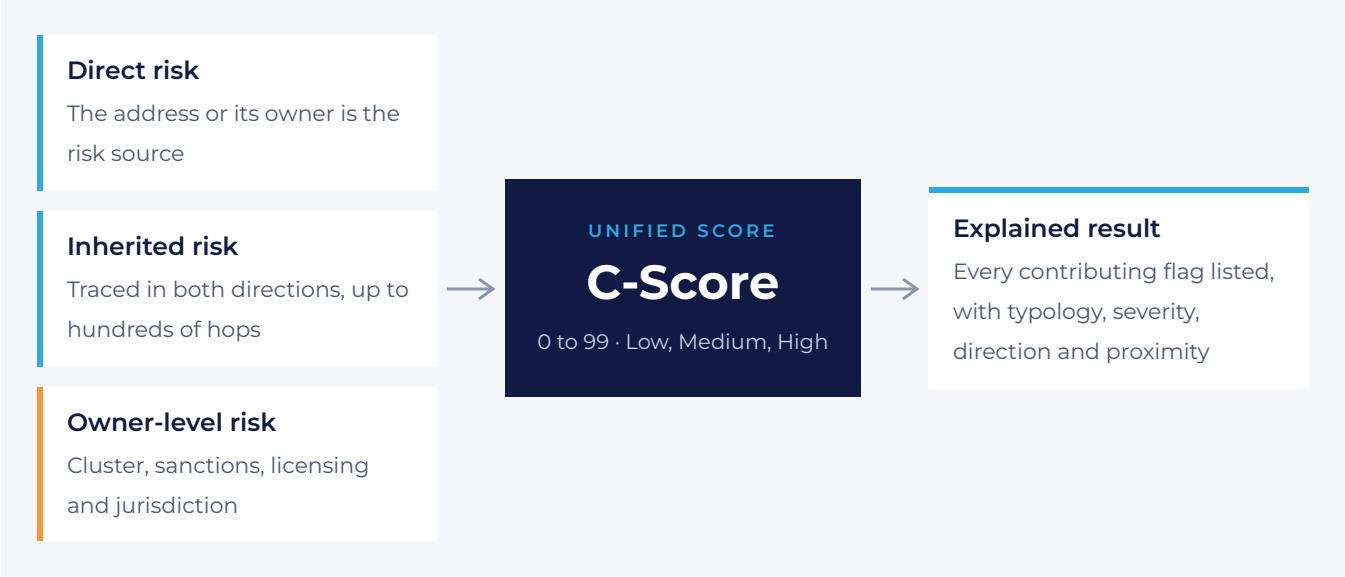
DIMENSION	COMMON SHORTCUT	LUKKA'S APPROACH
Scope	Scores the address in isolation	Address, inherited exposure and owner, merged into one score
Data integrity	Automated scraping; unverified reports treated as fact	Three sources, daily human review, multi-reviewer verification
Exposure logic	One hop, incoming funds only, binary yes or no	Up to hundreds of hops, both directions, weighted by share of turnover
Unknown addresses	No data defaults to low risk	No data starts at Medium (33); low risk is earned by evidence
Explainability	A single opaque number	Every score delivered with its flags, typology, severity and evidence
Configurability	Fixed vendor defaults	Flags, severities and 223 jurisdiction ratings aligned to internal policy

Source: Lukka Blockchain Analytics methodology.

Dimension 1: Scope

COMMON SHORTCUT	Score the address in isolation, based only on the transactions that touched it.
WHY IT FALLS SHORT	Risk does not live only in an address's own history. A newly created address controlled by a sanctioned entity has no illicit transactions at all. Screened in isolation, it looks clean.
LUKKA'S APPROACH	Every wallet is assessed across three dimensions at once and merged into a single risk score, the C-Score. Clustering links each address to every other address controlled by the same party, so owner-level risk such as sanctions status, licensing and jurisdiction applies to all of them.

EXHIBIT 2 | THREE DIMENSIONS OF RISK, ONE EXPLAINED SCORE



Source: Lukka Blockchain Analytics methodology.

Dimension 2: Data integrity

COMMON SHORTCUT	Rely on automated scraping alone, and treat unverified reports as confirmed.
WHY IT FALLS SHORT	Attribution errors become false positives that consume analyst time, or false negatives that let real exposure through. Evidence of illicit activity is also ephemeral: a source online today may be gone tomorrow.
LUKKA'S APPROACH	Three independent sources, collected automatically and by a dedicated team that reviews sources every day, with every data point checked by multiple reviewers before it enters the model.

EXHIBIT 3 | THREE INDEPENDENT SOURCES OF TRUTH

SOURCE	WHAT IT CAPTURES	SCALE
On-chain	Historical and real-time transactional data, ingested directly from blockchains as new blocks are created	108+ blockchains covered; 1.2B+ attributed addresses
Off-chain	Addresses linked to sanctions, terrorism, cybercrime, crimes against persons, dark-web activity and other predicate offences	~27,000 surface, deep and dark web sources monitored daily
Shared intelligence	Information from cooperating VASPs and partners on hacks, ransomware and other events that warrant flagging	Continuous

Source: Lukka Blockchain Analytics methodology.

Every finding is also labelled by its evidence basis. **Knowledge-based** findings are deterministic: who owns an address, which addresses cluster together, where funds moved, backed by retained evidence. **Risk-based** findings come from statistical and machine-learning models that detect behaviour aligned with FATF red flags, such as rapid movement of funds or structuring below reporting thresholds. Analysts always know whether a flag reflects documented fact or behavioural inference, which is exactly the distinction an examiner will probe.

Dimension 3: Exposure logic

COMMON SHORTCUT

Count only direct counterparties, look only at incoming funds, and treat any contact with a risky source as a simple yes or no.

WHY IT FALLS SHORT

Laundering is designed to add distance. One-hop screening misses layered flows. Incoming-only screening shows where money came from, but not where it went next. And binary logic flags a wallet that received a fraction of a percent of its turnover from a mixer the same as one funded entirely by it, flooding review queues with false positives.

LUKKA'S APPROACH

Inherited risk is traced from one hop to hundreds of hops away, in both directions, and weighted by the share of the wallet's total turnover connected to the risk source.

EXHIBIT 4 | EXPOSURE IS WEIGHTED BY MATERIALITY

PROXIMITY TIER	SHARE OF TOTAL TURNOVER	FLAG LABEL
First tier	20% – 100%	"Significant part" of incoming or outgoing transactions
Second tier	1% – 20%	"Part" of incoming or outgoing transactions
Third tier	Up to 1%	"Dust funds" taint

Source: Lukka Blockchain Analytics methodology.

Dimension 4: The unknown

COMMON SHORTCUT	If there is no data, assign low risk.
WHY IT FALLS SHORT	Absence of evidence is not evidence of low risk. A blockchain does not reveal who controls a fresh address, and creating addresses then leaving them dormant to build apparent tenure is a known illicit tactic. Treating silence as clearance is convenient for throughput, but hard to defend before a supervisor.
LUKKA'S APPROACH	An address with no data starts at 33, Medium. A low score must be earned by evidence, such as a licensed owner in a low-risk jurisdiction. Each of Lukka's 380+ risk indicators either raises the score, lowers it, or adds context without changing it, with severities set by AML/CFT and sanctions specialists against international AML/CFT requirements and FATF virtual-asset typologies.

EXHIBIT 5 | C-SCORE RISK LEVELS

LOW 0–32	MEDIUM 33–65	HIGH 66–99
Includes addresses where only risk-decreasing flags apply	Starting point: an address with no data, or only informative flags, scores 33	Highest-severity findings; blacklisted addresses are set to 99

Risk increasing
Severity 1–99; raises the score

Informative
Severity 0; context only

Risk decreasing
Deducted from the score

Source: Lukka Blockchain Analytics methodology.

Dimension 5: Explainability

COMMON SHORTCUT	Return a single number and a broad label.
WHY IT FALLS SHORT	An opaque score forces analysts to re-investigate from scratch, leaves the institution unable to explain its own decisions, and cannot be reconciled with any other system.
LUKKA'S APPROACH	Every C-Score is delivered with the full list of flags behind it, including typology, severity, direction and proximity. Teams can triage on the score and drill into the flags once a threshold is crossed, or act on specific flags such as sanctions regardless of the score. Supporting evidence is extractable, and every action taken in the platform is recorded in an audit trail.

Explainability also decides whether a score can travel between systems. Scores are not interchangeable: each provider uses its own scale, weights and labels, so a 70 in one model has no fixed equivalent in another. Labels diverge too. One provider's "mixer exposure" may be another's "privacy service." The two names can describe the same activity while signalling very different levels of concern, which matters on a Travel Rule network where each counterparty may rely on a different analytics provider.

What can be compared is the structure behind a finding: the risk category, whether exposure is direct, owner-derived or inherited, its direction, how many hops away the source sits, what share of turnover it affects, and whether the finding rests on attribution or behavioural inference. Lukka's flags encode each of these consistently, so they can be mapped across providers with reasonable fidelity, and a flag seen in a Travel Rule workflow means exactly what it means in the full Lukka investigation. A score that returns only a number and a broad label cannot be reconciled, because that information was never surfaced.

Dimension 6: Configurability

COMMON SHORTCUT	Apply the same vendor defaults to every client.
WHY IT FALLS SHORT	The risk-based approach under MiCA, the EU AML package and FATF guidance requires controls calibrated to the institution's own business risk assessment. A generic default cannot reflect an institution's licensing, products or geographic exposure.
LUKKA'S APPROACH	The Risk Assessment Model can be customised flag by flag: which indicators are active, how they affect the score, and how severe they are. Its 223 jurisdiction ratings, derived from seven sources including FATF, sanctions lists and the Basel AML Index, can be overridden to match internal policy. Whitelisting or blacklisting an address changes its score, but detection continues, so a trusted counterparty whose circumstances change still triggers alerts.

Taken together, these six choices determine whether a risk score is a control an institution can defend, or a number it has to explain away.

SECTION 2

Turning the risk score into a transaction decision

A risk score only protects an institution if it changes what happens to the transfer. CryptoSwift integrates blockchain analytics into the compliance authorization workflow, including Travel Rule, AML sanctions screening, and Enhanced Due Diligence operations. The rule engine lets institutions operationalize their risk policies, such as Lukka's risk assessment as a condition before funds are released.

EXHIBIT 6 | FROM RISK SCORE TO RELEASE DECISION

CRYPTOSWIFT	CRYPTOSWIFT	LUKKA	CRYPTOSWIFT	CRYPTOSWIFT
Know Your Wallet	**Counterparty VASP risk**	**Blockchain risk screening**	**Rule engine**	**Transaction monitoring**
Detect wallet type; route the right workflow	Assess the VASP on the other side	C-Score plus every underlying flag	Score as a condition before funds are released	Ongoing review after settlement

RULE ENGINE OUTCOMES	Released	Held for review	Escalated for EDD

Illustrative workflow. Configuration varies by institution.

How the rule engine uses the score

Because the C-Score arrives with every underlying flag, rules can work at both levels, mirroring how most compliance teams already operate:

- **Score thresholds.** Transfers below the institution's threshold proceed; transfers above it are held for review, with analysts drilling into the flags behind the score.
- **Flag-specific rules.** Certain findings, such as sanctions exposure or terrorism financing, can trigger a hold regardless of the overall score.
- **Counterparty context.** The counterparty VASP's risk score sits alongside the transfer's, so the decision about *whether to transact with this VASP* is made together with the decision about *this transfer*.

Every transfer ends in a documented, consistent outcome: released, held for review, or escalated for enhanced due diligence. Each outcome can be traced back to the specific score and flags that drove it, which is exactly what an examiner will ask to see.

Monitoring after settlement

Risk does not end when a transfer completes. A counterparty address that screened clean last month can receive tainted funds tomorrow. CryptoSwift's transaction monitoring, powered by Lukka, keeps reviewing activity after settlement, so changes in risk surface as alerts rather than as findings in an audit.

SECTION 3

Processing stablecoins: what changes

Stablecoins are increasingly how banks, payment firms and VASPs move value on-chain. That raises the bar on both sides of the workflow: transfers must be screened and resolved quickly, and the resulting positions must be valued and reported to an audit standard.

CryptoSwift: payment processing hub

- **Fraud prevention through Know Your Wallet (KYW).** CryptoSwift detects, with varying degrees of confidence, the wallet type behind a transfer. That determines which Travel Rule workflow applies, since a transfer to a hosted wallet at another VASP is handled differently from one to a self-hosted wallet. Transactions with other custodians require Travel Rule message exchange, while self-hosted wallets require proof-of-control. KYW can also be used as a signal to prevent fraud: a hacker extracting funds to a self-hosted wallet might declare it as a custodial one, and evade the required verification.
- **Enhanced due diligence on demand.** When the rule engine escalates a transfer, CryptoSwift can request source-of-funds and source-of-wealth information from the customer right in the transaction flow, instead of resorting to manual (e.g. e-mail based) workflows.
- **AML sanctions screening.** Travel Rule data is used for sanctions and watchlist screening as well as adverse media checks, which can be triggered from the CryptoSwift suite.
- **360° transaction overview.** CryptoSwift processes Personally Identifiable Information (PII) on payment counterparties, financial information, AML screening results, and the on-chain risk score. Users can also access the Lukka graphical user interface from the CryptoSwift transaction view for detailed inspection. In short, CryptoSwift serves as a natural hub for processing, investigating, and understanding transactions.

Lukka: risk scoring and accounting

- **Risk scoring.** Stablecoin transfers are screened with the same methodology described in Part 1, across the 108+ blockchains Lukka Blockchain Analytics covers. Lukka also tracks and normalizes 840+ stablecoin-classified tokens, so institutions know exactly which asset, on which chain, they are screening.
- **Accounting and valuation.** Once a stablecoin transfer settles, it becomes a position that must be priced, reconciled and reported. Lukka Prime provides Fair Market Value pricing aligned with GAAP and IFRS, and Lukka's data and reporting tools reconcile on-chain and off-chain activity into audit-ready records, under SOC 1 and SOC 2 Type I and II controls.

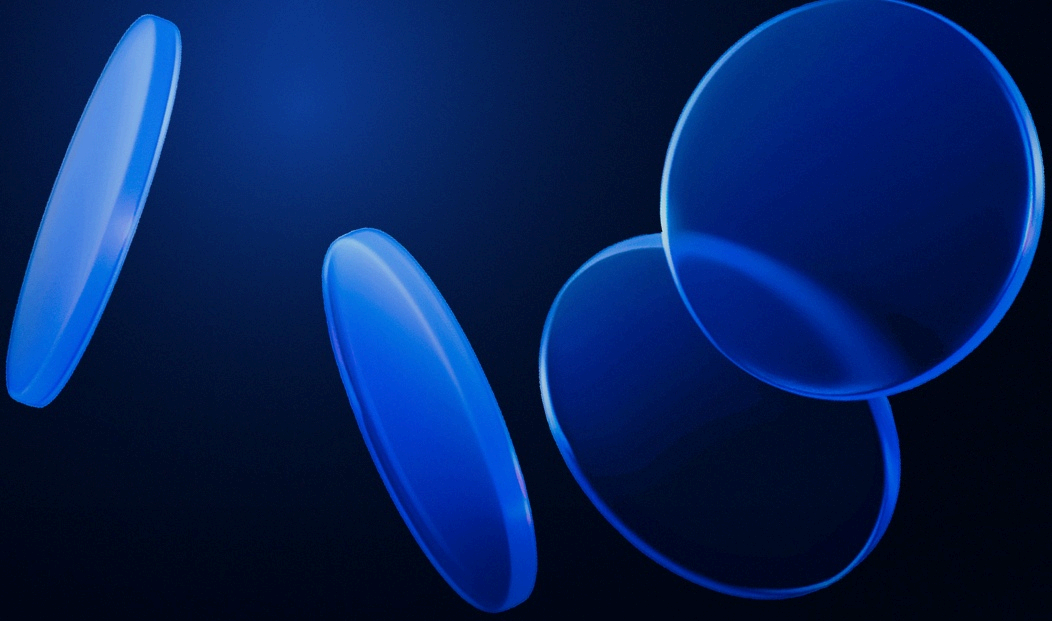
Together, that closes the loop: the transfer is screened and resolved before it moves, and the asset it creates is valued and reported to an audit standard after it lands.

CONCLUSION

The score is where the decision begins

With MiCA fully in force, the Travel Rule operational and the AMLR arriving in July 2027, the question supervisors ask is no longer whether an institution screens. It is whether the institution can explain what its screening concluded, and show what it did as a result.

That takes two things working as one. A methodology that measures risk on evidence, across the wallet, its flows and its owner, and explains every score. And a workflow that turns that measurement into a consistent, documented decision before funds move. Lukka and CryptoSwift together bring both to the institutions they serve.



TAKE THE NEXT STEP

The score is where the decision begins.

Lukka

See the methodology in action

Lukka Blockchain Analytics and Lukka Blockchain Investigator give compliance and investigations teams explainable wallet, transaction and entity risk scores, ongoing monitoring, and case management built for regulator-ready reporting.

lukka.tech/contact-us

CryptoSwift

Put risk scores to work in your Travel Rule workflow

CryptoSwift connects Travel Rule compliance with blockchain analytics, so every transfer is screened, decided and documented before funds move.

cryptoswift.eu/contact

DISCLAIMER

This document is provided by Lukka, Inc. and CryptoSwift for general informational and educational purposes only. It does not constitute legal, regulatory, compliance, tax, financial or investment advice. Regulatory references reflect the authors' understanding as of October 2026; laws and supervisory expectations change frequently and vary by jurisdiction. Readers should consult qualified legal and compliance advisers regarding their specific obligations.

Each company is responsible for the description of its own products. Descriptions reflect capabilities as of the date of publication and are subject to change without notice. Coverage figures are approximate and updated on an ongoing basis. Risk scores, flags, rules and related outputs are tools intended to support, not replace, an institution's own risk assessment and professional judgment. Neither company guarantees that any analysis will identify all illicit activity or that any particular regulatory outcome will be achieved. Example workflows and outcomes are illustrative only. References to other providers or approaches are general in nature and do not refer to any specific company or product.

© 2026 Lukka, Inc. and CryptoSwift. All rights reserved.