USE CASE

Fraud RFIs: Fund Recovery, Request, and Response

How real-time cross-bank coordination changes fund recovery outcomes.

The coordination problem

Three in four euros are gone by the time cross-bank collaboration begins.

That is not a technology failure. It is a structural one. The financial system moves funds in seconds. The institutions managing those funds still coordinate by email, phone, and SWIFT MT199 — tools designed for communication, not joint action. There is no shared case ownership. No structured context. No mechanism for synchronised response.

The result is predictable. Fraud is confirmed internally, escalated through compliance, routed to an external portal, and eventually reaches a peer institution — by which point the funds have moved on. Layered into crypto. Distributed across mule accounts. Gone.

The industry's default workflow is not a failure of willingness or effort. The tools the industry has relied on were not designed for the speed of modern criminals.

What Salv Bridge does

Most inter-bank fraud tooling is built around confirmed fraud. Bridge operates in the suspicion phase: before the transfer completes, before the funds move, before the window closes.

Investigators replace fragmented email threads with governed, auditable requests for information. Both institutions work within the same case. Context is shared in a structured format. Action is coordinated, not sequential.
By moving collaboration upstream, Bridge users recover funds that everyone else loses.

Bridge also supports AML investigations, sanctions screening RFIs, and proactive alerts that warn peer institutions about suspicious behaviour before a transaction is attempted. The same infrastructure handles each workflow.

Operational outcomes

Bridge has facilitated over 60,000 lawful intelligence exchanges across more than 100 financial institutions in 16 EU and UK jurisdictions since 2021.

Metric	Result
Median first-action speed	15 minutes
Customer losses prevented	~€3 million
Recovery rate, large Nordic bank (post-Bridge)	80% — up from 10%
Network cases with partial recovery	50%
Median true positive rate on shared signals	84%
Internal investigation time saved per alert	20+ hours

How it works

A fraud engine flags a suspicious event — such as an unusual transfer or a pattern-based alert — and routes it for human review. The investigator initiates a Bridge request from the interface, targeting a specific counterparty or broadcasting to the network. Where Bridge is integrated via API, the request is triggered automatically at the point of detection, without manual intervention.

Structured alert routing

The request arrives at the receiving institution immediately. Both teams work inside the same digital workspace, reviewing a structured alert with defined fields: beneficiary details, transaction chains, risk indicators. There are no forwarded emails. No version control problems. No lag.

End-to-end encryption

All shared intelligence is protected using a public/private key model. Messages are decrypted only by the receiving institution's private key — available via the Bridge UI, or held internally under a Hold Your Own Key setup for API integrations. Salv cannot read the payload. Neither can anyone else.

Templated information exchange

Data exchange is structured into predefined templates that enforce compliance with AMLR Article 75 and PSR Article 83. Role-based access controls and a full audit trail record what was shared, when, and by whom.

Coordinated action and closure

When the threat is resolved, both teams close the case with mutual confirmation. The outcome is logged. The audit trail is complete.

In practice: Estonia

Bridge is live across 100% of the Estonian banking market.

In one case, an analyst identified a customer attempting to wire funds to an overseas exchange — behaviour consistent with a coaching scam. The sending bank halted the wire. The customer then attempted to redirect the funds to a third institution.

The investigator opened a multi-conversation view in Bridge, queried the originating bank to confirm account history, and sent a structured alert to the third institution. Both receiving banks acknowledged the warning and placed targeted account restrictions. The funds did not leave the banking system.

A similar intervention recovered €100,200 from a corporate phone scam and was concluded in less than 20 minutes.

These are not edge cases. They represent what coordinated action looks like when the infrastructure exists to support it.

"Bridge proves that collaboration works. It helps us respond faster, protect more customers and, most importantly, build trust between people who once worked in isolation."

Siiri Graabi
AML/CTF Officer
Coop Bank Estonia

Why it compounds

Criminal networks are already operating across institutions. Fraud schemes move funds through multiple banks deliberately — because each institution only sees a fragment of the picture, and fragments do not trigger action.

Bridge changes the unit of analysis from a single institution to the network. When enough institutions share intelligence in real time, the fragmentation that fraud depends on disappears. The exit routes close.

Every institution that joins strengthens the signal. Response times tighten. Recovery rates increase. The harder it becomes to move money undetected, the less viable the scheme.

That is the argument for network-level infrastructure — not that it is better than bilateral coordination, but that bilateral coordination cannot work at the speed and scale that modern fraud requires. The criminals figured this out. The industry is catching up.

About us

Salv empowers financial institutions to beat financial crime with a SaaS platform that helps them detect money laundering, share intelligence, and stop fraud.

Criminals work in networks, so financial organisations should too. With the world's first fincrime platform that enables intelligence sharing, Salv helps banks, fintechs, and payment service providers fight financial crime more effectively and recover 80% more stolen funds.

More than 100 companies across Europe use Salv to centralise their AML data, exchange intelligence, automate repetitive tasks, and reduce false positive alerts. As a result, they can beat more criminals and protect their customers better.

Led by a team of crime fighters and data scientists who helped scale fincrime operations for Wise and Skype, Salv is a regulated partner and licensed KYC data processor on a mission to make the world a safer place by beating financial crime.

Our customers

LHV · TRUELAYER · coop Pank · zen · Bigbank · SEB · inbank · montonio · OP Bank · Luminor · rewire · KR · MONEVIUM

salv