USE CASE

Pooling Offboarded Customers

What happens when banks can query intelligence on terminated customers and suspicious entities.

The information gap bad actors rely on

When you terminate a customer for money laundering or fraud, they don't stop. They walk next door and open a new account. They move to the next institution, go through onboarding, and start again. Banks are often making that decision independently, with no visibility into what happened elsewhere.

Informal workarounds exist — reference checks between compliance officers, bilateral intelligence agreements, shared watchlists assembled by hand. None of them scale. They create inconsistent compliance records, depend on personal relationships, and cannot keep pace with how criminal entities move across the financial system.

Salv Bridge is the structured alternative. It is a lawful, production-grade mechanism for pooling and querying intelligence on high-risk and terminated entities across institutions in real time.

What it does

Institutions report verified terminations for severe financial crime risk — money laundering, fraud, and equivalent offences — into a shared encrypted pool. When onboarding a new applicant, your system queries that pool automatically. A match surfaces before the customer completes onboarding, giving your investigators the context to make an informed decision.

The primary use case is KYC and onboarding screening, but any unique identifier linked to suspicious activity — IBANs, devices, account numbers — can be reported and queried. That makes it a viable foundation for broader entity-level coordination across financial crime typologies.

In numbers

- **44%** of entities reported in 2025 were queried multiple times by different institutions within the same year, confirming that offboarded bad actors attempt re-entry across the network
- For every **500** bad actors stopped at onboarding, institutions collectively save or prevent a minimum of **€562,500** in fraud losses and recovery costs
- API integration reduces manual investigator effort on screening workflows by up to **70%**, primarily by eliminating ad-hoc lookup processes
- API integration expands screening coverage by up to **100 times** compared to manual look-ups, catching many more offenders

How it works

Reactive entity reporting

Participating institutions operate under a shared rulebook that defines reportable offence categories and minimum data requirements for submission. When a relationship is terminated for a qualifying reason, the institution submits a report: a sanitised entity record and a structured case description. The record is encrypted and pushed into the national pool. Raw identity data is never exposed to other participants.

For institutions requiring complete data sovereignty, a decentralised architecture is available. In this model, each institution retains full local control of its own data. Matching occurs without centralising records in a shared store.

Proactive querying

At onboarding, your system queries the pool against the applicant's details. A match returns the relevant intelligence: the offence category, behavioural signals from the reporting institution's case description, and sufficient context to decide whether to escalate due diligence or decline. A match is a signal, not a verdict. Final onboarding decisions remain with each institution, according to its own risk appetite.

Cryptographic privacy matching

Matching is double-blind. You cannot enumerate records in the pool or run speculative lookups. A match is only returned if you already hold the underlying entity data — the same identifier, to the same standard. Only an exact match unlocks the intelligence behind it. This applies to person identities, IBANs, device identifiers, and any other entity type in the pool.

On exact matching: this operates at the identifier level — document number, IBAN string, device fingerprint. Fuzzy name matching is not used, because it produces noise that compliance teams cannot act on reliably.

"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

How compliance teams use it in production

Adoption follows a consistent arc. Teams begin by querying the pool manually during due diligence, running lookups case by case or via weekly batch exports as a reference check alongside standard KYC. As confidence in match quality grows, institutions integrate via API and shift to automated, continuous screening.

Continuous portfolio screening

API integration means your existing customer base is screened against the pool on a recurring basis, at a frequency you configure. If a peer institution terminates one of your current customers for a qualifying offence, the next API run returns a match. Your investigators are notified and can initiate a review. You are not waiting for that customer to trigger an internal alert.

Human-in-the-loop reporting

Querying is automated. By design, reporting is not. The value of the pool depends on the quality of what goes into it. Investigators write structured, sanitised case descriptions — specific enough to give peer institutions actionable behavioural signals, stripped of any information beyond what is necessary for that purpose. This applies to all entity types. The human-in-the-loop requirement is not a limitation; it is a quality control mechanism and a compliance safeguard.

Data minimisation is enforced at the reporting stage. Institutions share what is strictly necessary for the receiving institution to make a risk decision. Standard templates support this in practice.

Demonstrable ROI

Embedding Salv Bridge directly into a bank's architecture via API integration increases onboarding screening coverage by orders of magnitude and reduces the manual overhead associated with ad-hoc intelligence workflows. The collective benefit scales with network participation: more institutions reporting means higher match rates and earlier detection across the system.

"When you're a bank, you want to know your technology partner will give you real attention. With Salv, we feel that. They understand how we operate and what we need to stay compliant and secure."

Mart Veskimägi
Head of Risk
BigBank Estonia

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 · deVere · Swedbank · JUNI · Citadele · Taptap Send · change · swile

salv