GUIDANCE

Intelligence sharing in financial crime: a guide to safe, compliant collaboration

Taavi Tamkivi
CEO and Co-Founder,
Salv

Why this guidance? And why now?

I don't need to tell you how money laundering or fraud happens. Or that it's increasing exponentially, while at the same time getting harder to spot.

Everyone in fincrime is on the same mission: to protect customers and stop criminal activity. Yet most teams at banks, EMIs, PSPs, and crypto firms still work in silos.
Not by choice. But because collaboration is operationally and technically complex. And most of us are already stretched working with the tools we've got.

Regulatory caution means that collaboration and intelligence sharing stay on conference stages; great in theory, rarely acted on.

But it's already happening.

Fincrime fighters compare notes over coffee, or send a "you might want to take a look at this customer" message to a former colleague.

That's intelligence sharing. Suspicion passed on quickly, with good intentions. But quietly, informally, and outside policy.

We created Salv Bridge to change that. To standardise this behaviour, make it safer, and bring it into the light.

It started five years ago as a request from an early Salv customer, who said: "I know this information is useful to another bank you work with. But I've got no compliant way to share it. Can you help?"

Since then, intelligence sharing has become our obsession. And Salv Bridge has grown into a cross-border network of more than 100 financial institutions, used in several countries across the EU and the UK.

These teams collaborate in real time. Sharing intelligence in a compliant, secure, standardised format that keeps everyone protected.

On the journey so far, we've learned that technology isn't enough. Real collaboration is built on trust. And trust grows when there's a clear, shared framework that explains how, when, and why to share intelligence.

Created for fraud, AML and compliance professionals, this guidance outlines the practical guidance we've developed to support you on your journey to safe, compliant and legal intelligence sharing. And a resource you can share with your legal colleagues, too.

It aligns with Article 75 of the EU Anti-Money Laundering Regulation, which supports structured intelligence sharing partnerships across sectors and borders. It considers both EU and national laws, along with our own experience facilitating hundreds of thousands of compliant exchanges.

The guidance is already being used in multiple markets to power real collaboration across a range of fraud, anti-money laundering (AML) and counter-terrorist financing (CTF) use cases.

Now, it's here to help more institutions get started.

I won't lie to you and say it's been easy defining a new category for heavily regulated financial institutions. But that doesn't mean better collaboration is impossible. It just needs the right structure.

Together with regulators and the industry, we've established guidance that joins the dots into something that actually works.

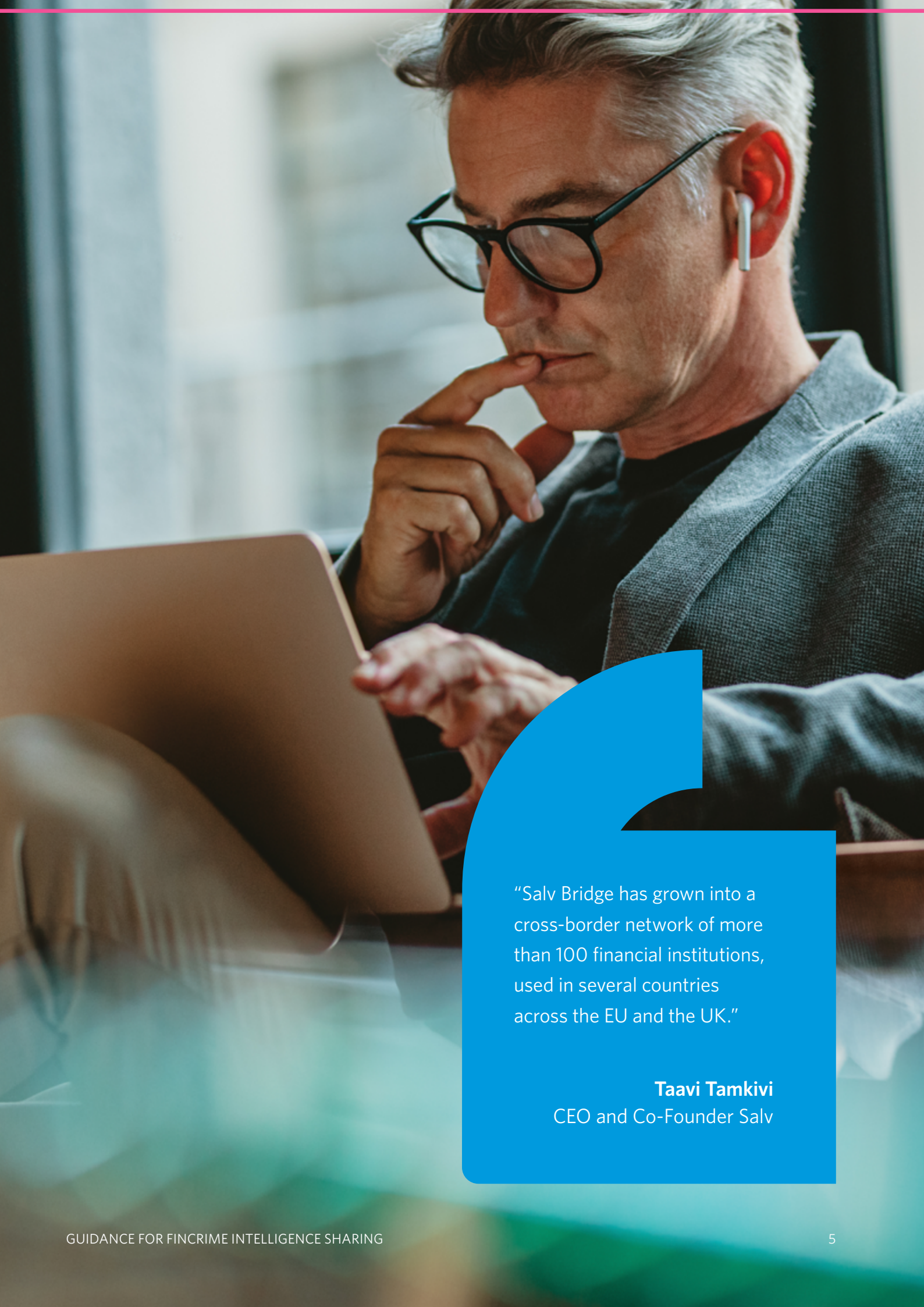
So as you read on, ask yourself: "what's actually stopping us?"

Because intelligence sharing is the next-generation of financial crime prevention. Hopefully, this guidance helps you take the next step.

If you have any questions, or want us to sense-check your approach, we're happy to share our practical experience.

GET IN TOUCH

Inside the guidance



"Salv Bridge has grown into a cross-border network of more than 100 financial institutions, used in several countries across the EU and the UK."

Taavi Tamkivi
CEO and Co-Founder Salv

Overview

This guidance defines the operating standards to ensure that intelligence sharing between financial institutions is conducted in a safe and compliant manner.

It provides a standard for good practice when collaborating and exchanging intelligence on fraud, AML and CTF. Obligated private entities, regulators and supervisors can apply this guidance to their relevant jurisdictions, confirming a legal basis for intelligence sharing and ensuring auditability.

This is a shared standard for use across the EU and the UK that translates EU laws and directives, jurisdiction-specific interpretation, and technical protocols into practical guidance that enables ongoing collaboration between financial institutions.

It's closely aligned with Article 75 of the EU Anti-Money Laundering Regulation, which sets out the conditions for partnerships for information sharing between obliged entities. In addition, it also reflects the standards established in the Latvian Data State Inspectorate's Closed Service KYC Utility. These references underpin the emphasis on strict necessity, data minimisation, cross-border cooperation, operational governance, and supervisory oversight.

It sets out to:

- Enable the secure, justified, and timely exchange of intelligence between directly involved financial institutions.
- Provide a structured and standardised approach for case-based collaboration across banks, electronic money institutions, payment service providers, and virtual asset service providers.
- Support a suspicion-based approach to intelligence sharing, with a focus on fraud and AML triggers, as opposed to bulk data sharing.
- Avoid unnecessary data exchange that would breach GDPR principles by enabling targeted, case-specific collaboration. Each institution retains control over its own data, and only suspicion-based intelligence related to a particular transaction is exchanged between counterparties.
- Ensure that all activity remains compliant with applicable legislation, including the GDPR, AML Directives, PSD2/PSD3, relevant national frameworks and national regulations derived from those named directives.
- Promote audit-ready practices that help institutions meet regulatory expectations and reduce reputational risk.

1 Guiding principles

Article 75(1) provides the foundation for these principles by stating that "members of partnerships for information sharing may share information among each other where strictly necessary" for the purposes of fraud, AML and CTF. This guidance adopts and operationalises this requirement. It's underpinned by the following principles:

Suspicion-led collaboration

Intelligence sharing must relate to a specific case where there is suspicion of fraud or money laundering.

Proportionality and necessity

Only the data necessary for the investigation or decision-making process should be exchanged.

Reciprocal duty to act

Institutions commit to responding in good faith to valid, well-scoped intelligence requests.

Security-first design

All exchanges take place on a secure, encrypted platform with access controls in place.

Auditability and transparency

As per Article 75(6), obliged entities must define policies and procedures for sharing information, including roles, responsibilities, and access controls. This principle ensures that all activity is logged and traceable, supporting both internal oversight and external regulatory review.

2 When and why to collaborate

The purpose of collaboration and intelligence exchange between regulated financial institutions is to prevent and reduce financial crime – including fraud, money laundering and terrorist financing – to ensure compliance with international sanctions, and to reduce the exploitation of the financial system for criminal purposes.

To achieve this shared purpose, financial institutions will send and receive intelligence via a sole platform, such as Salv Bridge, responding to requests in a timely manner while complying with the obligations and restrictions established by legislation and internal rules.

Institutions may exchange intelligence relating to transactions, circumstances, and customers identified as suspicious or high-risk. This enables financial institutions to send and receive alerts of suspected fraud or AML and investigate them further.

Before submitting enquiries to other financial institutions, Salv Bridge users will first apply necessary due diligence measures using their own internal tools, reliable databases, and public sources. Only once this has been completed should Salv Bridge users make enquiries and begin collaborating.

The legal basis for intelligence exchange between institutions is generally established through national AML and CTF legislation, which reflects EU-level directives but may differ by country. Institutions should consult Salv's separate legal analysis to understand how specific laws are applied in each jurisdiction.

Any exchange of intelligence with public sector organisations must comply with the relevant legal requirements, including those related to personal data protection and banking secrecy. For example, police authorities may request information in accordance with jurisdiction-specific legal rights.

As per **Article 75(2)**, participation in a partnership for information sharing requires prior notification to supervisory authorities and verification that appropriate safeguards are in place, including a completed data protection impact assessment (DPIA). This document guides obligated entities and relevant authorities on how to fulfil those conditions.

3 Deciding to share

The decision to collaborate and exchange intelligence is made independently by each institution using a shared technology platform, such as Salv Bridge. This assessment is based on applicable legislation, including rules on banking secrecy, personal data protection, and the safeguarding of business secrets; as well as the institution's internal procedures and any relevant collaboration agreements.

The intelligence shared must support clearly defined purposes - such as the prevention of fraud, money laundering, terrorist financing, or the enforcement of international sanctions - and its use must remain confidential and proportionate to those aims.

Intelligence vs information vs data sharing

In financial crime prevention, three things matter: regulations, technology, and people. But what connects them – and makes them effective – is knowledge.

It's easy to blur the lines between data, information, and intelligence. But they're not the same:

Data

Data is raw. Think transaction logs, IP addresses, or lists of names.

Information

Information is processed data. It might show a flagged transaction or trigger an alert.

Intelligence

Intelligence is what actually helps you act. It's context-rich, judgement-led, and tells you what to do next.

Most teams aren't short on data or alerts. What they're missing is intelligence. And that's where human insight makes the difference.

4 Technology and controls for operational success

Effective intelligence sharing requires more than legal permission: it also depends on having the right technological infrastructure in place.

Article 75(4) outlines safeguards required for information sharing, including pseudonymisation, recording of activity, and information minimisation. To meet these operational conditions, all intelligence must be exchanged through a platform that protects any information or documentation transmitted electronically using encryption to ensure security and confidentiality.

This includes:

- End-to-end encryption and role-based access to structured case information
- Predefined templates and safeguards to ensure data minimisation and relevance
- Full activity logging of every exchange, fulfilling Article 75(4)(a)

Each institution should define:

- Internal Standard Operating Procedures (SOPs) and escalation flows that define when, why, and what to share, fulfilling Article 75(6)
- Named users and their roles, including differentiated access and the controls to support limited access to sensitive information, fulfilling Article 75(6)(a)
- Retention and deletion protocols for downloaded/shared data

Purpose-built platforms such as Salv Bridge are designed to operationalise this guidance, adhering to all of the above safeguards. Salv Bridge enforces strict suspicion-based sharing logic and template-based input, ensuring that each exchange remains proportional, relevant, and audit-ready in line with the expectations of Article 75.

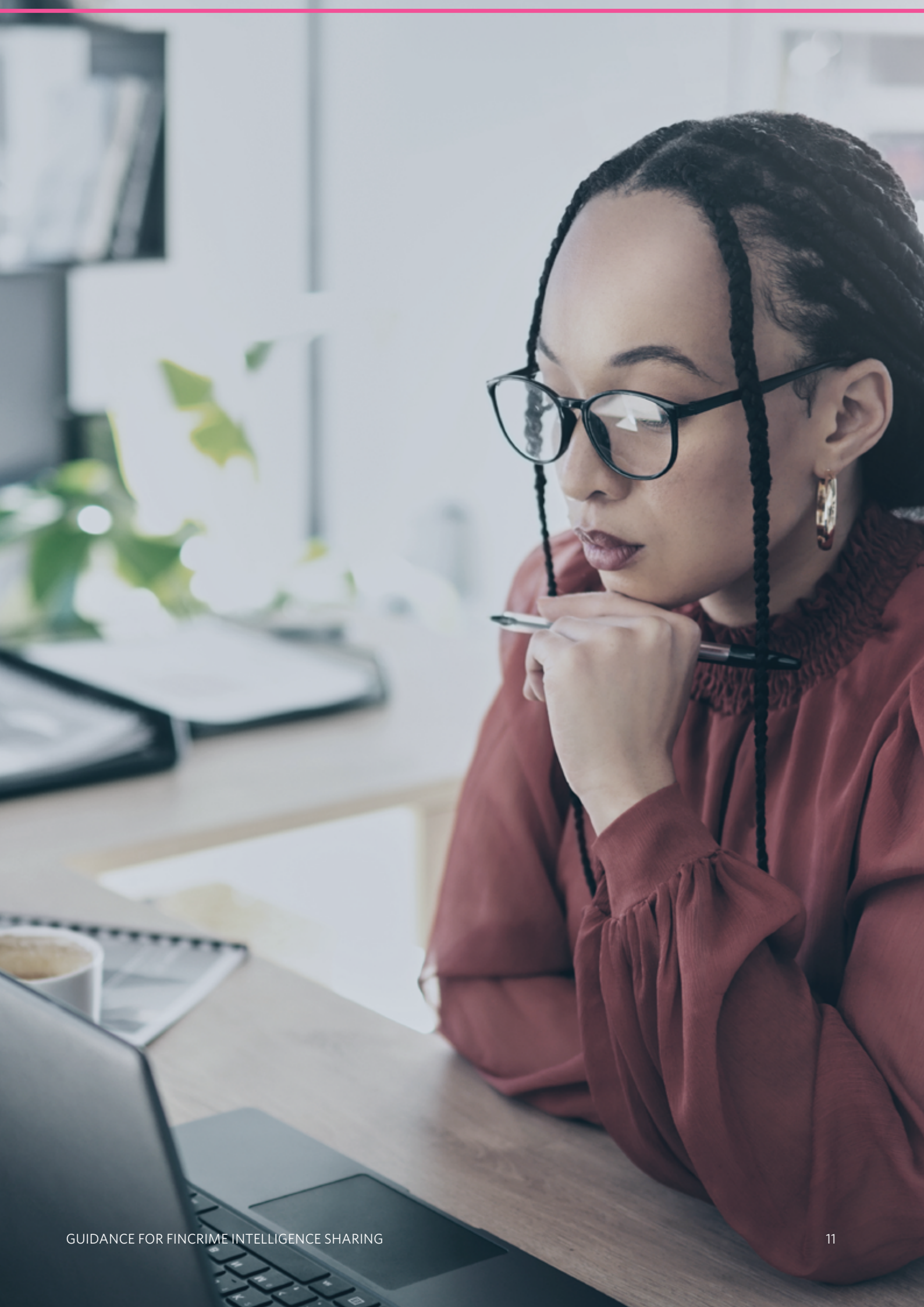
Article 75(7) further allows supervisory authorities to request independent audits. Platforms must have an architecture that enables internal oversight and external review as part of ongoing compliance, such as Salv Bridge.

Article 75(1) not only permits information sharing between obligated entities, but also supports such exchanges across borders, recognising that financial crime is inherently cross-border. Intelligence sharing platforms must be designed with that scalability in mind, incorporating regulatory awareness, legal flexibility, and operational standardisation from the outset.

This guidance provides the consistency needed to support the evolution of intelligence sharing across Europe, regardless of the technology platform an institution chooses to adopt. Salv Bridge offers a proven and audited pathway for meeting supervisory expectations and already supports compliant intelligence sharing in several EU jurisdictions. While not required, it is a proven way to bring this guidance to life in practice.

If you'd like to discuss how to operationalise this in your organisation, get in touch.

GET IN TOUCH



5 What kind of intelligence can be shared

Article 75(3) outlines the types of information that may be shared in the context of a partnership for information sharing. This includes customer identity, transactional details, risk factors, and suspicions. The following categories align with that scope and may be shared via the platform, depending on each financial institution's use case and internal compliance framework. Not all categories need to be made available to all end users; access and visibility are defined by each institution's internal policies. Additionally, new and more specific data types may be introduced, provided they are approved in accordance with the institution's internal compliance procedures.

List of data exchanged:

- **Client-related data:** Full name, registration number or personal identification code/date of birth, contact details, and data on related parties. Such as representatives, beneficial owners, politically exposed persons (PEPs), company owners, card users, internet banking users, and other associated individuals. This may include supporting documents, declared information (e.g. main partners), and details on the origin or source of assets or wealth.

- **Transaction data:** Date, amount, purpose or explanation, IBAN, counterparties' names, and information on the source or destination of funds.

- **Relationship-related intelligence:** Information about the refusal or termination of a business relationship, including data on standard or exceptional account closures.

- **Due diligence challenges and elevated risk factors:** Cases where due diligence measures could not be completed or where risk is increased, for example, due to adverse media, unverifiable or missing data, concerns around the information provided, cash-related risks, or links to shell companies.

- **Fraud and other criminal activity:** Details of suspected fraud, including identity fraud, forged documents (e.g. account statements, payslips, IDs), tax fraud, or other financial crimes. Specify the type of suspected fraud where possible.

- **Sanctions-related intelligence:** Links to sanctioned individuals or entities (e.g. through ownership or control), or geographic connections to sanctioned regions, whether formally documented or otherwise identified.

- **Data related to dual-use goods or weapons of mass destruction:** Information relevant to due diligence, suspicion of money laundering or terrorist financing, or international sanctions.

- **Non-personal strategic intelligence:** Alerts on emerging risks, typologies, or trends to support early detection, simplify investigations, and raise collective awareness. May include supporting documents where appropriate.

As per Article 75(5), information received through a partnership must not be further transmitted except under specific conditions restricted by system safeguards and internal policies.

6 Request standards and response timelines

Requests for intelligence must be well-founded and purposeful. Each request must clearly state its objective - for example, confirming a suspicion or identifying links between individuals and suspected criminal activity.

Requests are appropriate to:

- Investigate transactions suspected of involving financial crime.
- Understand the risk profile of high-risk clients, including those subject to enhanced due diligence.
- Clarify inconsistencies in customer-provided information or investigate suspicious activity on an account.
- Determine the origin of funds or potential links to terrorism or its financing.
- Prevent fraud by sharing intelligence on suspected fraudsters or known victims.

Requests should be limited to cases where additional information is essential for decision-making. For instance, when there is reason to believe that a customer's account was previously closed under exceptional circumstances.
Before sending a request, users must assess its justification and define the scope of the required intelligence in accordance with sections 2 and 5 of this guidance. Upon receiving a request, the recipient will review its justification and may ask for further clarification if needed.

Responses must supplement, not replace, internal decision-making. Article 75(4)(b) specifies that institutions must not rely solely on received information to fulfil regulatory duties.

When preparing a response, only the intelligence outlined in sections 2 and 5 of this guidance should be shared. Institutions must avoid sharing data that may interfere with another institution's due diligence processes or decisions related to account openings or closures. Responses must refer to actual transactions identified in account statements and may include the legal basis or contextual justification for the request.

Deadlines

- Urgent requests (e.g. those concerning financial sanctions screening, fraud prevention, or processing of time-sensitive payments): response required within 1 business day or immediately in cases of ongoing fraud prevention.
- Standard requests: response required within 3 business days.
- If additional time is needed, the responding institution must inform the requester and provide an estimated timeline for response.

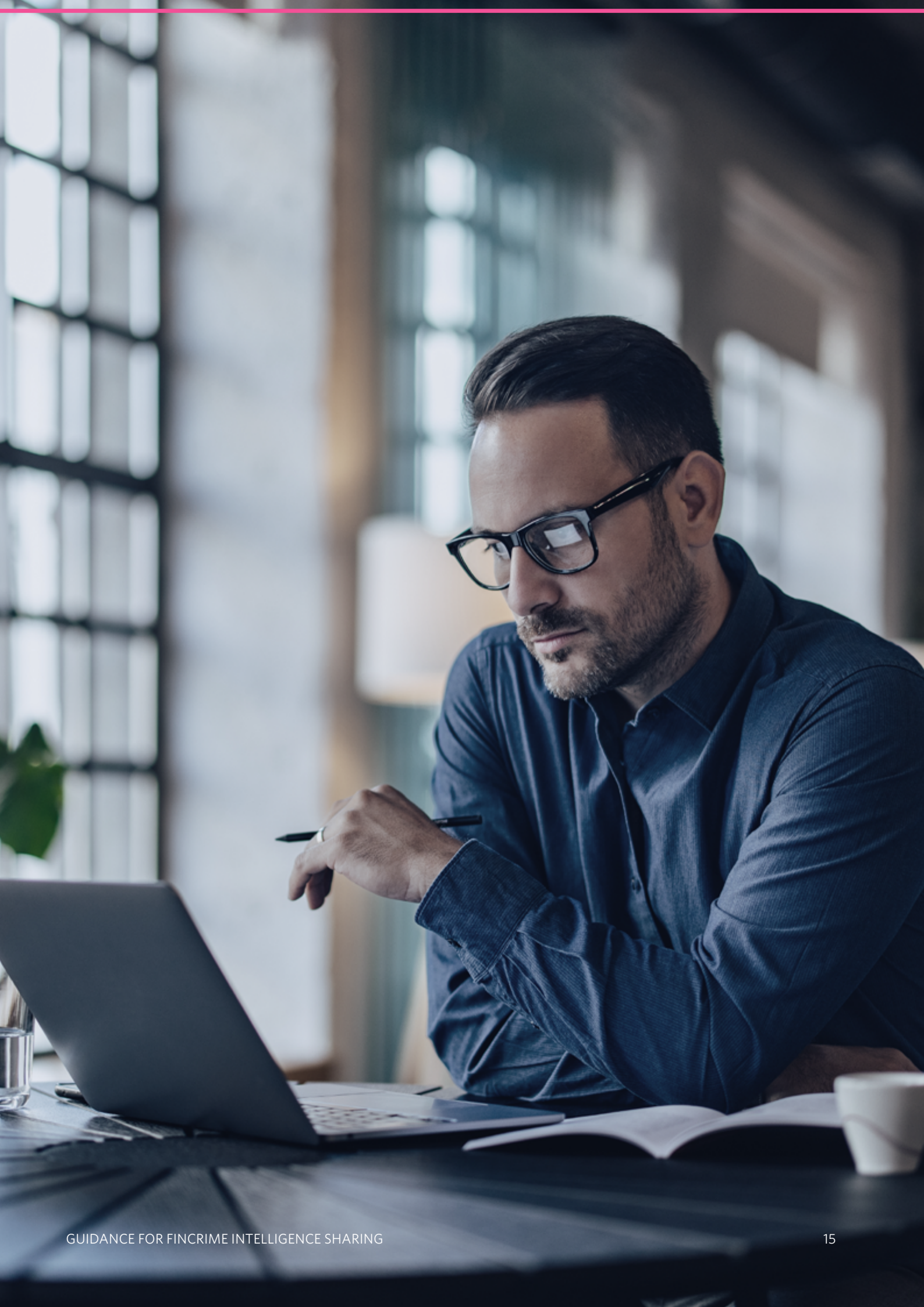
7 What makes a request unjustified

A request will be considered unjustified in the following cases:

- There is no evidence that the customer has a relationship or history of transactions with another financial institution, or no due diligence measures are applicable.
- The request does not concern a high-risk customer, is unrelated to enhanced due diligence, or does not involve suspicion of financial crime.
- The information requested concerns the status of a current customer relationship without relevance to due diligence obligations.
- The request appears commercial in nature or pertains to the client's general activity, without a clear link to financial crime prevention or risk clarification.
- The request is excessive or vague in scope, such as:
  - Requesting a full account statement when only the origin of assets for a single transaction is needed.
  - Asking for all transactions between entities or above a certain threshold without clear justification.
- Requesting the full history of due diligence measures when the context involves institutions outside the EEA or the UK.

If you want to take the next step, such as a pilot, benchmarking exercise, or exploratory call, we're happy to chat.

GET IN TOUCH



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 · zen · Bigbank · SEB · inbank · montonio · OP Bank · Luminor · rewire · KR · MONEVIUM · deVere · Swedbank · JUNI · Citadele · Taptap Send · change · swile

salv