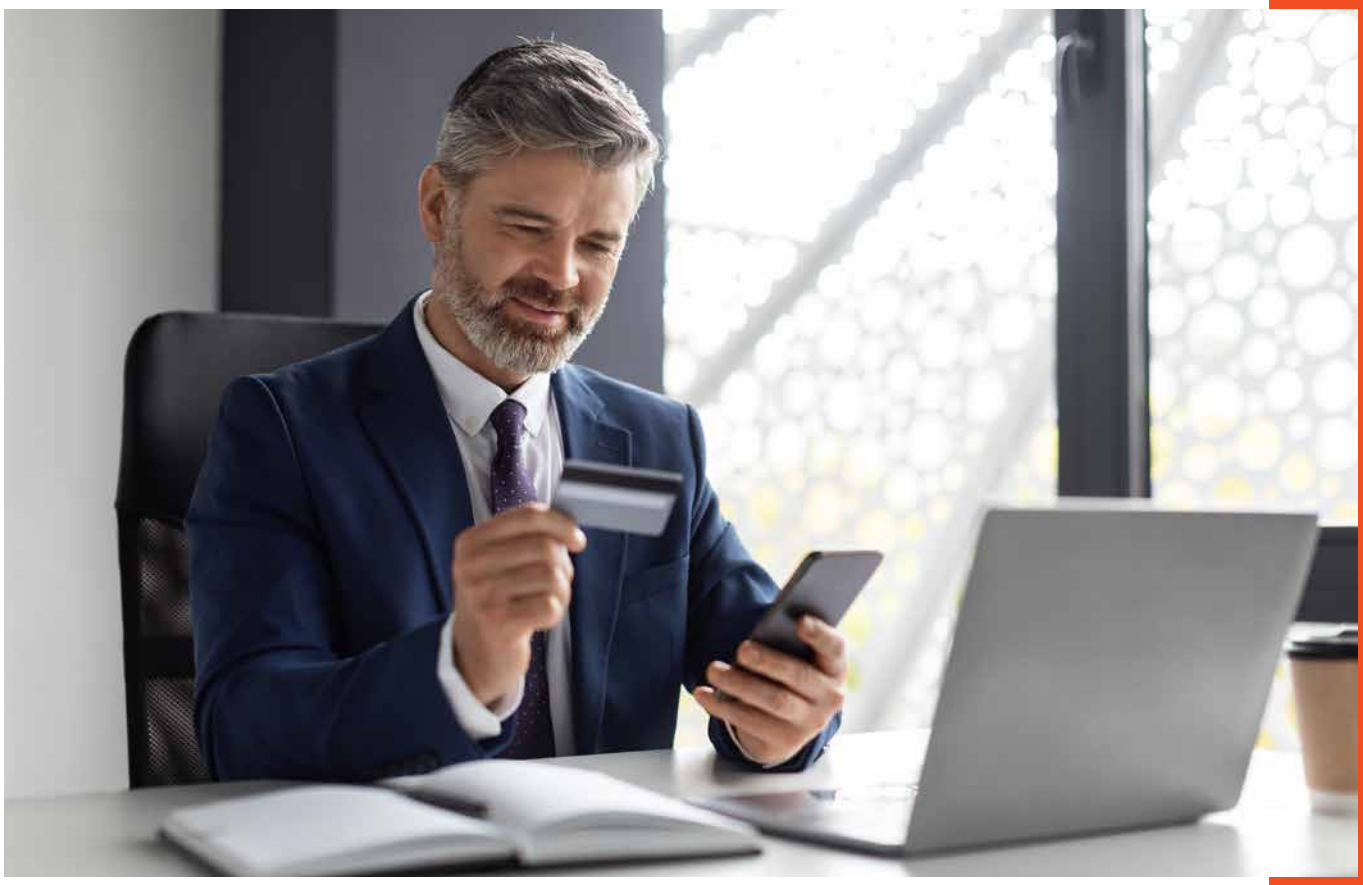
# Three lines of
# ID FRAUD DEFENSE

**a protocol to help risk & compliance leaders in banking and financial services**



## Executive brief

If you want to prevent cascading financial, regulatory, and reputational damage, this document is for you. We're explaining step-by-step how our Three Lines of Defense gives you the language and framework to move the ID check conversation from "cost of compliance" to "strategic safeguard of integrity." And why the leaders who take ID authentication beyond the compliance checkbox will be the board members of tomorrow.

KEESING Technologies

**Verify with trust. Protect with confidence.**

# Introduction

In situations where one wrong ID verification can lead to catastrophic loss,
***"good enough"* ID verification is no longer good enough.**

If you are responsible for risk mitigation, compliance or security in high-stakes financial services such as wealth management, capital markets or payment security, you live in this reality every day.
You don't simply want to tick a regulatory box, you are defending the integrity and reputation of your organization. And then, you're also required to ensure a good onboarding experience for new staff or customers.
We created this vision document especially for you. It's a sketch of a near-future in which verification of banknotes and ID documents is not a weak link, but a strategic strength: flawless, defensible **and designed for people who can't afford to be wrong.**

Let us inspire the future of ID authentication with our

## Three Lines of Defense Protocol.

Jan Lindeman
CEO Keesing Reference Systems

*Dec 11, 2025*

# 1 Your margin for error is disappearing

Read any fraud report and you'll find that volumes and complexities of ID documents, data sources and fraud patterns increase. More cross-border transactions and remote onboarding expose you to risks of sophisticated document forgery and synthetic identities.

At the same time:

- Operational teams need efficiency
- Customers expect instantaneous decisions
- Product teams want smooth onboarding journeys
- Regulators, auditors, the media and your board require more scrutiny

Speed and accuracy – traditionally enemies – are both non-negotiable.
So, how do you balance all those interests?

## The personal weight of responsibility

Truth is that there's quite a group that feels this pressure, but in a different way and based on their specific roles ar responsibilities:

- **Head of Compliance / Chief Risk & Compliance Officer**
  You're end-responsible for KYC, AML and fraud prevention. Your signature is on the policy, your name and career are on the line when an incident happens.
- **VP KYC / Director of Due Diligence**
  You own the flows and tooling. When a bad actor slips through or a good customer is blocked, it's your process that is questioned.
- **Head of Digital Onboarding / IAM Lead**
  You balance friction against risk. Make the journey too heavy and growth suffers; make it too light and exposure explodes.
- **Head of Digital Transformation / Innovation Lead**
  You are expected to unlock new digital channels without increasing risk. You need technology that is future-proof and easy to integrate into core systems.
- **CISO / Head of Security**
  You defend data, systems and integrations. Every new vendor and data feed is another potential point of failure.

What you all share is this: **you can't afford to be wrong**. Not once, not at scale, and certainly not in a way you can't defend or explain afterwards.

# Why "ticking the box" is the real risk

ID verification should be more than just 'ticking the box'. However, many ID verification processes are there to satisfy a regulation, but will not withstand a forensic investigation or a headline crisis. Risks are accepted. On paper. As long as it's not the newspaper.
Another uncomfortable truth is that exactly this box-ticking culture is the biggest reason that by mid2025 AML fines had already amounted to $6 billion worldwide, on its way to the costliest year on record.

## Typical tickbox patterns we see (and you might recognize):

- **Black-box algorithms** that give you a score, but not the why.
- **Fragmented tools** across channels, countries and product lines.
- **Third-party and extrapolated data** that you cannot see into or fully explain.
- Workarounds and expertise that live in people's heads, **not in your core systems.**

If you recognize any of the above, it shows that you're relying on mathematical probability instead of evidence-based determination, and siloed knowledge and point solutions instead of an ecosystem of expertise.

It may look compliant, but in reality, it raises at least three strategic risks:

1. **Compliance risk** – you are accepting probability where regulators increasingly demand certainty, evidence and traceability.
2. **Operational risk** – your teams spend time reconciling systems, handling exceptions and explaining why something is "good enough".
3. **Reputational risk** – when fraud or a sanctions breach hits, it won't be your hardware, software or data provider in the media or in front of parliament; it'll be you.

**These risks can be mitigated by implementing our Three Lines of Defense Protocol. Based on 100+ years of experience and government relations, it provides certainty over verification processes and ensures document authentication with maximum trust.**

# 2 A vision of flawless ID verification

Imagine an IDV foundation that's built deliberately for organizations and people who can't afford to be wrong. Organizations like yours. People like you. Not as a checkbox measure, not as a 'first line of defense' but as a means of evidence-backed control and trust.

## Defense Line 1: Data you can defend

The first layer is **first-party data, 100% accurate and complete.**
Instead of relying on probabilistic models based on the median of a thousand 'quite similar' ID documents (or in plain English: guesswork), safeguard your verification with a reference database that is verified daily and populated with document templates directly from issuing authorities and document manufacturers.
For you, this means:

- When an auditor asks, "Where does this reference data come from?", you have a clear, defensible answer.
- Every record is verifiable and every check traceable – no scraped, recycled or extrapolated data.
- Compliance becomes more than a policy statement; it becomes real.

And yes, at Keesing we have this level of (first-party) data accuracy and completeness.
**No ifs, buts and maybes**, only absolutes.

## Defense Line 2: Knowledge, not just calculations

The second Lines of Defense is forensic expert authority.
AI and automated checks are powerful, certainly. But high-stakes decisions still need human expertise. Research shows that roughly 15% of all cases need escalation. But to whom do you escalate?
In a flawless ID authentication world, you have access to an (internal or external) team of forensic ID document experts who know every security feature and every forgery method. Even at gunpoint, at 3 am.
If you're looking to outsource that level of expertise, Keesing offers investigative and consulting services, based on 100+ years of relationships with governments, document manufacturers and law enforcement agencies like the FBI and Interpol. If you want to stand your ground with regulators, courts or journalists, we have your back.

## Defense Line 3: Software that spots risk before it spreads

The third layer in the Protocol is efficiency and pacing.
The first two lines of defense can feel robust but also slow or frustrating for customer onboarding. They don't have to be. We see enterprises that implement the Three Lines of Defense Protocol reporting significantly less friction between accuracy and speed. Both for automated and manual ID checking.
For this third layer, here are some questions to ask yourself when considering IDV software that's fit for purpose:

- Does it have flexible APIs to integrate into my core systems?
- Can it serve both front-line and investigative teams in their jobs-to-be-done?
- How easy is it for operational teams to access and 'look-feel-tilt' the reference data?
- Is it a SaaS with proper configuration options for local regulations and policies?

If you have precision data at the speed of SaaS, you can catch anomalies before they enter your systems and spread through your organization.

# A noticeable change in predictability and certainty

Truth is that there's quite a group that feels this pressure, but in a different way and based on their specific roles and responsibilities:

**Resilient Reputation: don't just comply with regulations; defend the integrity of the organization you serve, and the financial system.**

**No Surprises: when incidents do occur, you can demonstrate controls were robust, based on best-available data and judgment.**

**Easy Audits: An audit? Great, you have clear evidence, traceable decisions and a consistent global standard to back you.**

**Great Onboarding: make customer experience a competitive edge: fast for legitimate customers, unforgiving for fraudsters.**

**Supported Checkers: Fraud teams that don't have to choose between speed, service and safety are better fraud teams.**

# 3 From today's reality to tomorrow's standard

Moving towards flawless ID verification is a strategic shift in how you think about identity risk. But strategic shifts are more impactful when made together. Here are 4 steps of how others have embraced the Three Lines of Defense as their new control system.

## Step 1 Reframe the problem

ID verification is not another line item in the compliance budget, it is a core control for institutional integrity.

Ask:

- Where would one wrong verification create catastrophic loss?
- Which processes are currently protected by probability, not evidence?
- Where do you rely on expertise that is not captured in your systems?

**This conversation belongs at the executive level – not just in a project steering group.**

## Step 2 Consolidate around a defensible data foundation

Audit your current data sources and tools. Identify where you are depending on third-party or opaque data, and where you lack traceability.
Then start rebuilding a framework what verification could look like around first-party, verifiable data. Start in your highest-risk segments (e.g. high-value clients, politically exposed persons, or high-risk geographies).

**Our Forensic Document Experts team is ready to help you out if needed.**

## Step 3 Add expert authority where it matters most

Not every case needs an authorized expert. But your organization needs **access to expertise** when things escalate. Either internal or external. Or both.

Build clear routes for:

- Escalations on suspicious, high-value or politically sensitive cases.
- Independent second opinions when internal teams disagree.
- Training for internal teams to raise their own detection capabilities.

**This is how you move from "we think this is fine" to "here is why this is defensible."**

## Step 4 Embed certainty everywhere in your onboarding journeys

Finally, connect this new foundation into your systems and channels:

- Identify fragmented tools that could be swapped with something more integrated.
- Standardize policies and rules across domains and geographies.
- Give front-line and investigators tools that surface the why, not just a pass/fail score.

**Wherever identity is checked in your organization, it needs to be 100% trusted.**

# No more sleepless nights, everybody wins

Truth is that there's quite a group that feels this pressure, but in a different way and based on their specific roles and responsibilities:

**Compliance & Risk get the defensible foundation and audit trail they need.**

**KYC team get consistent high-quality checks with confidence.**

**CX team get fast, reliable verification that creates happy customers at scale.**

**Digital Transformation gets a strategic platform, not another point solution.**

**Security gets confidence in data flows and storage, and robust integrations.**

# Why now?

Regulators are tightening standards, fraudsters are professionalizing, and digital channels continue to expand.
The organizations that treat ID verification as a strategic control instead of a cost of doing business will be the ones that:

- Avoid the worst crises.
- Win the trust of regulators and partners.
- Move confidently into new markets and channels.

And the people who lead that strategic control will be the board members of tomorrow.
If you are part of that group, this is your opportunity:
Move away from box-ticking compliance towards **certainty you can stand behind** – in front of your board, your regulator, media and the people you protect.

We'll be alongside you. All the way.