The value of a robust identification system is immense

The penalties for negligence in identity verification and anti–money laundering measures can be substantial. Fines amounting to hundreds of millions of euros for financial institutions are not uncommon, and employers risk €30,000 per employee who starts work without a proper ID check. Yet the gap between legal requirements and practical implementation remains wide.

Jan Lindeman,
Managing director, Keesing Technologies

Many organizations still view identity verification as a box to tick, rather than as a crucial component of business continuity and reputation management. Jan Lindeman, managing director of Keesing Technologies, recounts the story of a cleaning company with a constantly changing workforce from abroad that initially used a very basic verification product. After receiving a significant fine, they switched to the Amsterdam-based company's more extensive solution. "During the very first weekend after implementation, we intercepted 18 forged documents," Lindeman says. The value of a robust verification process became instantly clear, and there was no longer any debate about an investment of a few thousand euros compared with potential fines running into the hundreds of thousands.

Active worldwide

Keesing Technologies operates globally in identity verification and fraud prevention. The company has its roots in Keesing Publishers and has over a century of expertise in classifying official documents. That knowledge has evolved into digital, real-time ID-verification technology supported by a reference database containing nearly 14,000 official documents from hundreds of countries. Keesing receives these documents directly from issuing authorities, ensuring both accuracy and completeness. This database also forms the first line of defense in the three Lines of ID Fraud Defense protocol developed by Keesing.

Major U.S. banks

Four of the ten largest U.S. banks are Keesing clients, as are the country's largest credit card company, its biggest online marketplace, and dozens of other blue-chip firms. In the financial sector, Know Your Customer legislation is a major driver of advanced verification technology. Banks want to avoid doing business with Russian oligarchs or other suspicious parties. As noted, sanctions for negligence are severe. Lindeman: "A report published in June this year indicates that we have likely already passed the peak in fines for insufficient anti–money laundering measures."

"Often, when our sales team speaks with a bank about a solution, they say it's too expensive. But it's easy to counter that by asking: what does it cost when you're fined repeatedly?" Lindeman explains. It quickly outweighs the potential damage of inadequate controls.

Interestingly, the motivation is not only compliance. Efficiency plays a major role as well. In Norway, where all banks use Keesing's solutions, adoption was originally driven by a major fraud case fourteen years ago. But the biggest impact turned out to be the time saved in customer interactions. It illustrates a familiar tension: speed and convenience versus thoroughness and compliance.

In practice, the automated check using Optical Character Recognition fails in a significant number of cases. Documents may be wrinkled or dirty. In five to ten percent of cases, verification is forwarded to the back office, where human experts complete the check within two to three minutes on average. "In 99 out of 100 cases, it's not a forged document," Lindeman clarifies. "It's simply an error in reading."

That human layer remains essential. Keesing employs document experts – its second line of defense – who regularly attend international conferences to strengthen ties with government agencies and gather new reference documents. They are often former military police officers who can detect and document key security features with photos and descriptions. "They literally examine documents with a magnifying glass. It's a highly specialized skill."

Identification requirements: a blind spot

For employers with a rapidly changing workforce, the legal obligation to verify identity upon hiring is a growing risk factor. The law requires that an employee's identity be established on day one. "That often doesn't happen, or only roughly around that date. And usually not by trained staff with the right equipment," Lindeman notes.

The labor inspectorate can impose fines of up to €30,000 per violation. "If you're a company like Coolblue or Ahold, with thousands of employees, that adds up quickly." Many organizations only become open to a proper solution once the first fine arrives.

> *They really examine documents with a magnifying glass*

Sectors with high turnover, such as retail, construction and staffing, are particularly vulnerable. On construction sites, liability also plays a role: if an accident occurs involving someone who is not legally allowed to work, the legal and reputational damage far exceeds the initial fine. Large corporations like Siemens and Volkswagen use employee cards with built-in verification, but for many SMEs, identity verification remains an afterthought.

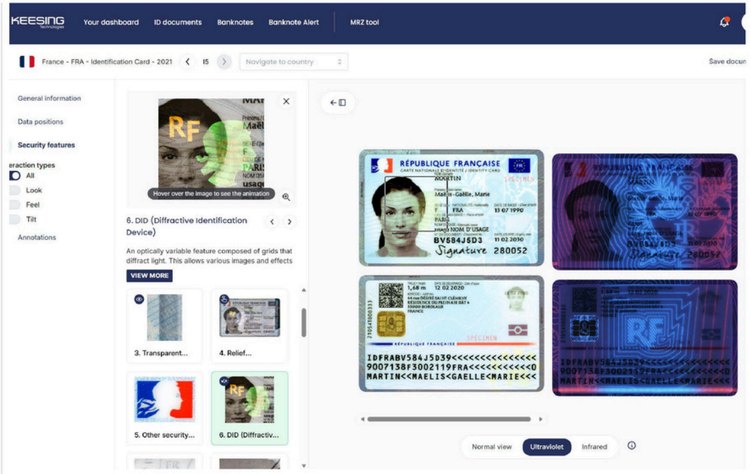
Europe leads the way

In the United States, the adoption of verification technology lags behind Europe. "There is still a great deal of manual, face-to-face verification," says Lindeman. That makes Keesing's reference database even more valuable. Identification in the U.S. is also more complex: each state has its own ID card, and some cards do not meet federal standards yet are still valid forms of identification.

"If you operate in the U.S. and a European customer wants to open an account, or someone from another state, you often won't know what that document should look like. What should you check?" For front-office staff without specialist training, that's nearly impossible.

Keesing's main differentiator in the U.S. is its reference database. They once relied on a physical booklet, but now they offer a digital platform with a multitude of documents. "The database is essentially a digital light table, allowing you to greatly increase image resolution." This is the advantage of the third line of defense: a software solution that anti-fraud teams can use easily and integrate via API into core systems.

The passport of the United Arab Emirates, for example, is one of the most advanced documents in the world, packed with subtle security features. Keesing's database shows in high resolution what these details should look like under various conditions –ultraviolet light, infrared, or when tilting the document. For Japan alone, the database contains 35 document types, from passports to driver's licenses.



Example: document from the Keesing DocumentChecker

> *What's your backup plan if online verification fails?*

This level of document knowledge is difficult to automate. "We see some competitors trying to use AI for this. But the customers who come to us specifically do not want the generated information to end up in an AI model," Lindeman emphasizes. Privacy and control over sensitive identity data therefore remain top priorities.

The fight against deepfakes

The rise of deepfakes and AI-generated identities requires additional verification layers. Keesing's solution combines multiple methods: seeing the person, reading the chip, and comparing the chip photo with a live image. "The most secure documents – passports – contain a chip. That's the ICAO standard," says Lindeman. The chip stores a photo and biometric data, among other things.

Reading such a chip requires the MRZ code, the machine-readable zone at the bottom of the document, or the CAN number, combined with a certificate. This technological lead is the result of nine to ten years of expertise in chip reading. It is a continuous process of tracking new documents and security features.

More than technology

For leaders in Risk & Compliance, the challenge extends beyond choosing the right technology. "It's about balancing efficiency and security, about designing the entire process. Besides technology, the people doing the work are a crucial factor in protecting your integrity," Lindeman stresses.

Training is therefore essential. Keesing provides not only data and technology but also training for staff performing identity checks. "We don't just teach people how to use our solutions, they're intuitive for most users anyway. We primarily train them on what to look for during the verification process. We're not only improving the checks but also the checkers."

Audit trails are another vital element. "Our service audit isn't just a report of data; it includes images of documents." These documents can be destroyed immediately after verification if the client prefers; the software is GDPR-compliant. But the audit trail must be available for regulators or for follow-up investigations. It is also important to show where the reference documents came from: directly from government authorities.

Cowboys in the market

Lindeman warns of "cowboys" entering the market. "Some parties quickly piece together an ID-verification system, but the final ten percent – GDPR compliance and data security – is often overlooked. Clients must be able to trust that they're sharing sensitive data with reliable partners."

Another issue is the illusion of automation. "What is presented as an automated process often turns out to be manual work," Lindeman explains. "OCR software and chip readers frequently fail, for example, when a document contains no chip. Then a back office steps in, performing manual verification based on photos. They often use our reference database for this. To the user, it feels automated, but behind the scenes a team of people is checking documents."

> *It's about finding the balance between efficiency and security*

Scenario thinking

Scenario planning is becoming increasingly important. How do you respond to deepfake threats? What is your backup plan if online verification fails? The solution often lies in hybrid models: online verification where possible, physical backup when needed. And distributed verification points for cases where people cannot come to an office. Organizations must therefore understand their risk exposure and determine the appropriate verification depth.

"It's really important to recognize the scale of the challenge," Lindeman says. "That's why we take on these kinds of projects. How do we help the people whose core responsibility is Risk & Compliance?" The answer does not lie in technology alone, but in consciously choosing the right balance between ease of use, efficiency, and watertight verification based on accurate data and deep expertise. A choice that can save organizations from tremendous damage.