Operating at the Speed of Crime

The Case for Real-Time Risk Intelligence

LSEG RISK INTELLIGENCE

Foreword

In 300 B.C., in what is largely considered the first recorded financial crime, a Greek merchant named Hegestratos failed spectacularly in his attempt to commit fraud. His scheme was to secure insurance on his ship and cargo, then sink the ship and sell the cargo elsewhere. Unfortunately for him, he was caught in the act of sinking the ship by his crew and drowned attempting to escape.

Criminals have grown considerably more sophisticated and unfortunately more successful since the time of Hegestratos. Today, banks face attacks on average every 14.4 minutes, and the cost from the damage of global cybercrime is expected to reach US$10.5 trillion in 2025. That's roughly US$29 billion per day and by 2031[1] some estimates suggest cybercrime will cost the world US$1 trillion per month.

Our 2025 LSEG Risk Intelligence Global Survey reveals other challenges for financial institutions. Regulatory scrutiny in the sanctions space is intense, and the consequences of non-compliance can often include severe financial penalties and potentially irreparable reputational damage. Yet simultaneously, these firms are still challenged by client demands for a seamless, reliable, accurate and rapid experience. Delays contribute to financial losses as well as loss of customer trust and expose firms to regulatory penalties and compliance overhead.

As we explored these challenges deeper, several key themes emerged, notably that inefficiency and compliance delays are plaguing our industry, but these challenges can be addressed with access to quality, real-time data combined with AI and workflow automation. We invite you to review the complete findings of the 2025 LSEG Risk Intelligence Survey as well as our recommendations for how financial firms can sharpen their ability to respond to financial crime threats with agile and resilient tools.

1 CyberCrime Magazine, January 31, 2025.

David White
Global Head of Product and Data
Risk Intelligence, LSEG

About the research survey

In mid-2025, LSEG Risk Intelligence surveyed 850 senior decision makers with responsibility over risk intelligence in financial institutions including top tier banks, wealth and advisory, banking (retail and digital) and investment (asset management and insurance).

Our survey included a wide range of countries and jurisdictions including:

- APAC (250): Australia, Hong Kong, Japan, Malaysia and Singapore
- EMEA (400): France, Germany, Italy, Nordics, Spain, Switzerland, UAE and UK
- North America (200): Canada and USA

Key findings

Our recent research survey of 850 senior risk and compliance leaders at top tier financial institutions reveal how compliance teams are adapting to real-time risk, identify barriers to adoption and explore the future role of human judgement in an increasingly AI and automation-driven compliance environment.

1. **Customer screening inefficiencies are widespread:** 80% of financial institutions reporting delays at least occasionally, causing persistent onboarding and payment delays.

2. **Operational inefficiencies are hindering effective customer checks:** 77% citing manual review workload as a major challenge and 75% reporting high false positives.

3. **Real-time access to sanctions and risk data is critical:** 98% considering it important to their compliance workflows.

4. **AI and workflow automation are essential to improving customer screening efficiency and effectiveness:** However, firms view automation and AI as complementary to human input, improving efficiency without replacing judgment.

5. **AI should enhance not replace human input**

Overall, findings show that AI, workflow automation, and real-time data access are key enablers of more efficient, accurate, and responsive customer screening processes, but expertise provided by human teams shouldn't be overlooked.

80% of respondents said delays happen at least occasionally, and nearly third of them face them often.

Customer Screening Challenges

Industry plagued by widespread delays

All financial institutions surveyed reported experiencing delays in their onboarding and payment processes due to compliance screening. Specifically, four out of five (80%) said these delays happen at least occasionally, and nearly a third (31%) face them often. For 6% of institutions, delays occur every single time.

The type of screening process used is related to the frequency of delays.

> Manual processes are particularly inefficient, with delays occurring every time for 10% of institutions that rely on them.

> Advisory firms are hit the hardest, with 14% reporting constant delays. This is notable because a higher percentage of these firms (59%) use a mix of manual and automated functions, compared to the 46% average across other financial institutions (insurance, bank and investment / private equity).

Mid-size firms with annual revenues between $250 million and $749 million, are also disproportionately affected. A significant 8% of these firms report delays always happening, and 40% say they occur at least often.

Operational, technological and data quality pose the biggest challenges in screening

Financial institutions face three main categories of challenges when screening customers for sanctions, PEPs (Politically Exposed Persons), and adverse media.

Operational burdens

Majority of financial institutions struggle with the need for manual review and remediation workload (77%) and managing a high number of false positives (75%). These findings highlight the considerable time and resource demands on teams, driven by high volumes of alerts and the need for human intervention.

Technology and integration limitations

Technology-related issues are also major hurdles. Three-quarters of institutions face issues integrating new tools (75%) with existing systems and dealing with inflexible software (67%). Additionally, some financial institutions noted delays in data updates (64%). This suggests current IT systems and tools may not be fully aligned with operational needs, leading to inefficiencies and slower screening processes.

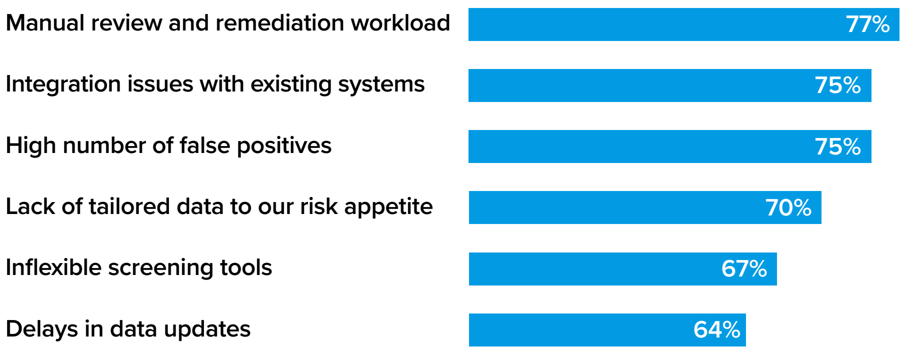
Data quality and relevance

A final challenge is the quality of data itself. Seven out of ten respondents reported that the data they receive isn't properly aligned with their specific risk needs, making it harder to accurately assess a customer's risk. This points to a misalignment between the information provided by current screening solutions and the precise data financial institutions require for effective risk assessment.

While these issues are generally consistent across the industry, their impact varies by sector. Once again, advisory firms are disproportionately affected (81%) as are insurance firms (80%), particularly compared to banks (61%). Insurance firms also experience a higher incidence of delays in data updates compared with the overall average (75% versus 64%).

Across all markets there's widespread challenges when screening on sanctions, PEPs, and adverse media

What are the biggest challenges when screening customers on sanctions, PEPs, and adverse media



Advisory and insurance firms face significantly higher challenges with inflexible screening tools (81% and 80% respectively). Insurance firms also experience significantly more delays in data updates (75%), perhaps due to lower levels of automation in their screening processes.

But a greater shift to workflow automation could solve these issues

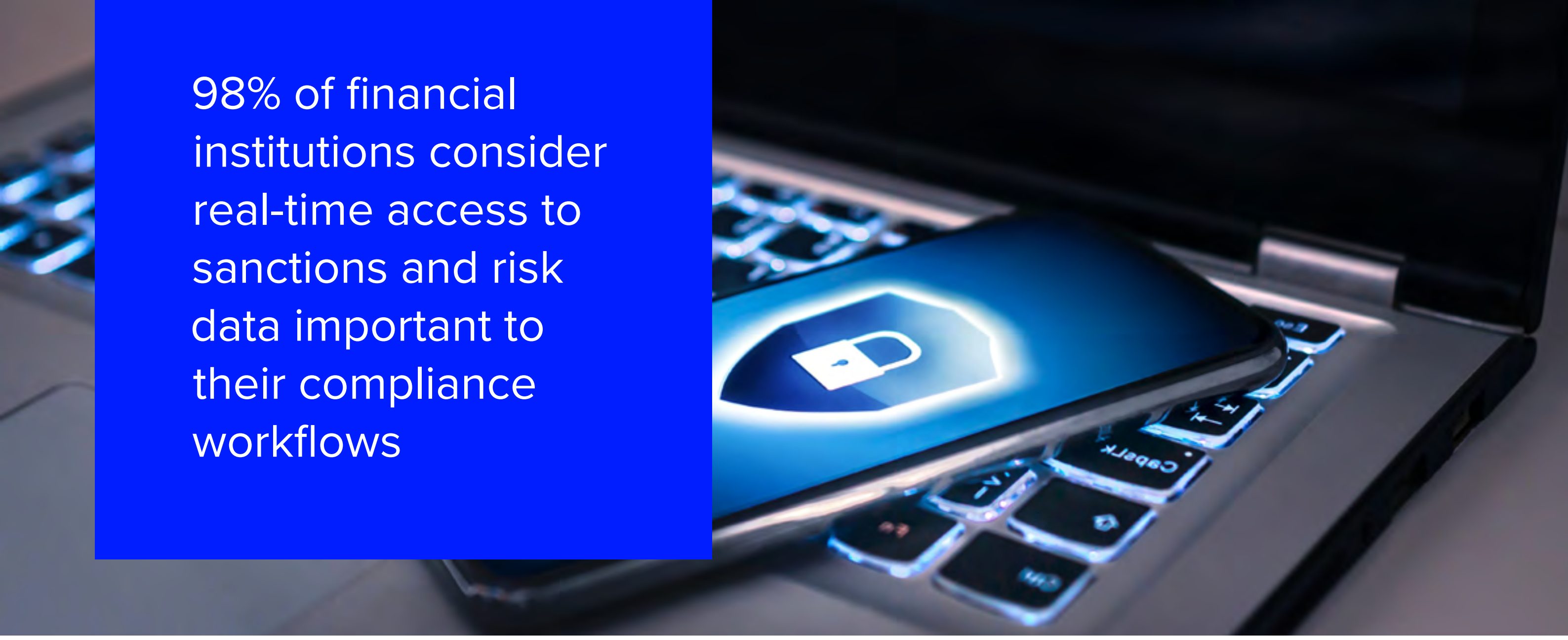
Integration issues with existing systems are significantly less of a challenge for financial institutions that rely primarily on automated screening processes (67%), suggesting that shifting more of the screening workflow away from manual processes could improve outcomes.

What's interesting to note however, is that institutions that use manual-only screening processes were less likely to report integration issues than those using a mix of manual and automated (77% versus 80%). This may point to the inherent complexity of mixed-model systems, frictions in workflow or lack of a single unified platform (i.e. legacy systems with automated software added later).

Similarly, integration issues are less common among financial institutions that outsource screening entirely to third parties, but noticeably higher for those using a combination of in-house and third-party providers (61% versus 77%, respectively).

Tailored data may also benefit from workflow automation. Financial institutions that rely mainly on automated customer screening are significantly less likely to report a lack of data aligned to their risk appetite as a challenge (65% versus 70% overall).

Similarly, workflow automation could be influencing confidence in risk screening data quality. Over half (54%) of financial institutions that rely on automated screening processes reported being 'very confident' in the accuracy of their data, compared with 43% across those that use only manual or a mix of manual and automated functions.



98% of financial institutions consider real-time access to sanctions and risk data important to their compliance workflows

Customer screening needs

Real-time data access is critical to compliance workflows

Real-time access to key data is the most critical factor for financial institutions. The survey revealed that this was the top consideration when selecting a screening tool for over half of all respondents (59%).

Overall, almost all financial institutions surveyed (98%) said real-time access to sanctions and risk data is important to their compliance workflows, with 62% rating it as very important.

Real-time data access provides a range of benefits especially around speed and efficiency

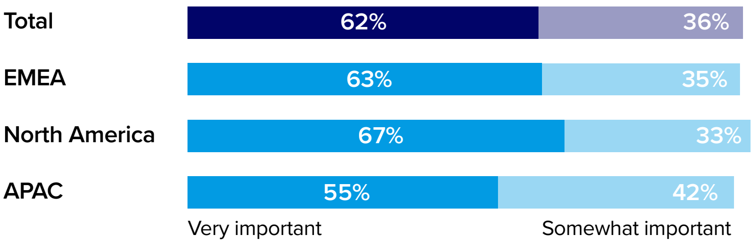
Why real-time data access is an important factor when considering a customer screenning tool

These factors were important across all markets and financial institutions. Insurance specifically benefited from speeding up customer onboarding (58%) and in APAC real-time data access had a significantly greater impact on lowering manual review workload when compared to other markets (44%).

When asked which single factor would persuade them to switch providers, respondents were most likely to choose real-time data access (21%). This feature is particularly influential among advisory and insurance firms (both 26%) and among mid-sized financial institutions (those with annual revenues between $250 million and $749.9 million), who are significantly more likely (at 25%) than average to switch for this reason.

Real-time data access to key data is overwhelmingly important to compliance workflow specially those using automation

Importance of real-time access to sanctions and risk data in current compliance workflows



Real-time access is important across all financial instituions, but those already using automated processes place significantly greater importance on it than those conducting manual checks. 69% say it is very important, compared with 54% respectively.

Benefits: managing risk in real time

The biggest advantages of real-time data are seen as managing risk in real time. It helps financial institutions avoid outdated data (49%), monitor risk continuously (48%) and manage fast-moving risk more effectively (48%).

Enabling compliance and regulatory alignment and improving operational efficiency and customer experience are also recognized as important benefits.

Importance of real-time data by region

While financial firms across North America, EMEA and APAC broadly aligned on the importance of real-time data, select differences do emerge. However, a closer look at real-time data access shows its significance varies across markets and segments:

In **EMEA** 63% of respondents rated it as very important, however:

- In the UAE, this rises sharply to 88%, and it is especially valued by functions managing regulatory and compliance risk (71%) and by companies with $750m+ in revenue (73%).
- Smaller companies and markets such as Italy were less likely to rate it as very important (53% and 44%, respectively).

In APAC, Malaysia and Australia, two-thirds (66% and 62%, respectively) consider it very important, compared with just 34% in Hong Kong.

- When selecting a customer screening tool, real-time data access emerged as the most influential factor overall (62%), particularly in Malaysia (72%) and Australia (70%).
- In Hong Kong, however, customisation to risk appetite and achieving greater precision with fewer false positives (both 54%) were viewed as more influential than real-time access (48%).
- Real-time data access is also the single factor most likely to drive switching providers, cited by 22% of respondents overall, rising to nearly a third (32%) in Japan.

Financial institutions **in North America** broadly align with other regions in viewing real-time access to sanctions and risk data as important for their compliance workflows, however:

- Real-time data access is critical to compliance workflows, but less so in Canada
- When selecting a customer screening tool, real-time data access emerged as the most influential factor in the USA (67%), but this drops to 45% in Canada.
- In Canada, workflow automation and support (54%) and ease of integration (52%) are more influential, likely reflecting the greater reliance on manual processes in this market.

Challenges: cost and the need for human input

Despite the benefits, several factors still hold financial institutions back:

Budget or resource constraints make real-time tools unfeasible for 45% of those who did not view them as an important factor, though this is a far less common reason among private equity and investment firms (35%).

40% of financial institutions said that manual review is required regardless of data speed, highlighting the ongoing need for human input even when automation is in place.

Outdated technology also plays a role, with 38% reporting that their existing systems are not built for real-time processing.

Readiness for the EU Instant Payments Regulation (IPR) is a high priority

Attitudes toward real-time data adoption are promising, especially in relation to IPR, which mandates that payment service providers in the European Economic Area (EEA) offer instant credit transfers in euros.

Overall, 72% of respondents say that readiness for the IPR is a high or top priority:

- 20% of all institutions consider it a top strategic priority, with significant time and resources allocated.
- 52% of all institutions report it as a high priority, balanced alongside other compliance initiatives.
- Banks show the highest level of emphasis, with 76% rating it at least a high priority.
- Insurance firms are more likely to consider it a moderate priority with 31% dedicating limited resources.
- Institutions that primarily rely on manual processes for compliance screening are significantly more likely to classify it as a top strategic priority with substantial time and resources allocated (27% versus 18% of those that rely primarily on automated or mixed processes).

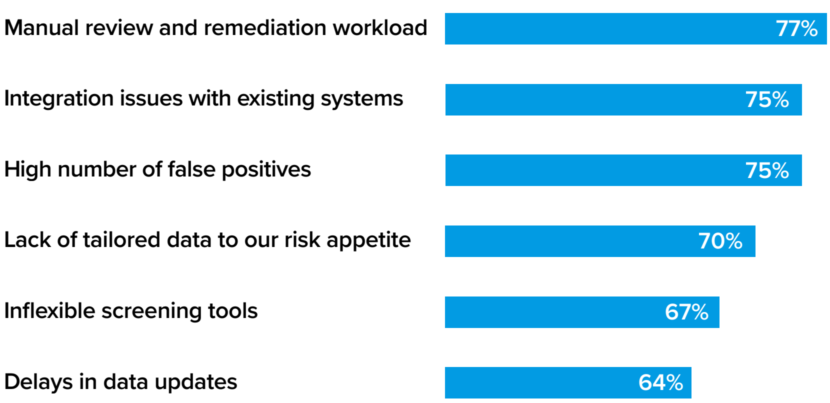
Better precision and fewer false positives are also important to the customer screening process

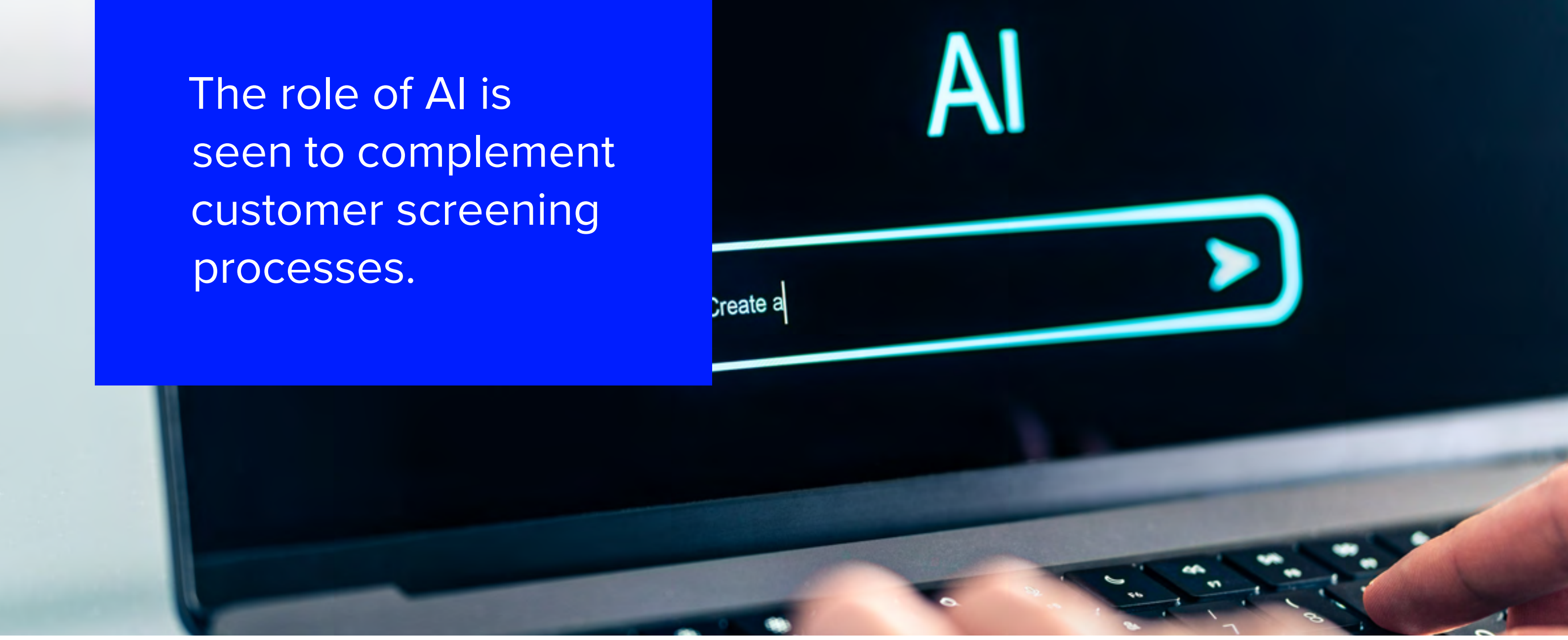
Beyond real-time access, other important factors when selecting a customer screening tool include:

- Better precision and fewer false positives. This was cited by nearly half of respondents (47%) as an important factor, and 18% as the main reason they would switch providers.
- Automation and workflow support was cited as important by 54% of respondents.
- Ease of integration was highlighted by 51% of respondents.

These features are particularly valued by banks, with 58% prioritising automation and workflow support and 54% highlighting ease of integration.

Biggest challenges when screening customers on sanctions, PEPs, and adverse media





The role of AI is seen to complement customer screening processes.

Customer screening solutions

AI and workflow automation set to transform customer screening

When considering improvements to the effectiveness of the risk screening process, financial institutions identified automation and AI integration as key priorities, with 21% highlighting this as a focus area. Respondents provided a range of examples, from enhancing real-time analysis and identifying fraudulent patterns to automating the verification of customer compliance documents.

However, financial institutions feel strongly that AI should enhance not replace human input

Several respondents emphasised that AI's role is to complement, rather than replace, the customer screening process, particularly by handling initial tasks.

Recommendations for financial institutions

Invest in real-time data, but know what you are buying

As financial crime accelerates in complexity and speed, investing in real-time data and advanced screening technologies is no longer optional – it's imperative. But technology alone won't solve the challenge. The true differentiator lies in choosing partners and data sources that align with your institution's unique risk appetite, operational realities, and long-term compliance strategy.

Real-time data is becoming more widely available, but the devil is in the details. Some solutions have data models with outdated risk intelligence or batch updates that delay responses to emerging threats. Other risks include newer solutions that may be faster, but often compromise accuracy, context, and structure, leading to over screening and heavier remediation workloads.

Based on our global research survey, we would recommend financial institutions to consider the following when choosing risk intelligence partners:

1

Prioritize data quality over quantity

Not all risk data is created equal. Firms must seek providers who deliver highly curated, structured, and context-rich intelligence – not just voluminous alerts. Precision matters: well-classified, granular data minimises noise, reduces false positives, and allows your teams to focus on genuine risks. Ask vendors about their data sourcing, update frequency, and how they ensure relevance to your specific geographic and sectoral exposure.

2

Demand transparency and adaptability

Look for vendors who offer clear visibility into data changes and seamless integration into your workflows. Real-time updates are critical but so is understanding what changed and why. Flexible, API-driven architectures that can evolve with emerging regulations, new payment rails, and shifting compliance requirements future-proof your investment.

3

Embrace a collaborative vendor relationship

Compliance is not a one-way street. The best partnerships involve continuous dialogue, customization, and joint problem-solving. Vendors should act as extensions of your team, proactively identifying emerging risks and tailoring solutions to your evolving risk landscape – not just selling off-the-shelf products.

4

Integrate AI thoughtfully to augment human expertise

AI and workflow automation unlock scale and speed, but human judgment remains indispensable. Adopt an AI strategy that emphasizes transparency, explainability, and human oversight – ensuring technology supports, rather than replaces, your compliance experts. This balanced approach mitigates risks inherent in automated decisions, such as bias or false positives, and strengthens your institution's ethical framework.

5

Embed real-time screening into a broader risk culture

Finally, technology and data should be integrated within a risk-aware organizational culture. This means aligning compliance processes with business objectives, investing in ongoing staff training, and fostering a mindset of agility and vigilance. Real-time screening is a critical tool, but it delivers its full value only when combined with skilled analysts empowered to act swiftly and decisively.

In summary, selecting the right risk intelligence partner means looking beyond speed and coverage but also to value, trust, adaptability, and partnership. Institutions that embed these principles in their vendor relationships and operational models will be best positioned to stay ahead of financial crime and regulatory scrutiny in the years to come.

LSEG Risk Intelligence provides a suite of solutions to help organisations efficiently navigate risks, limit reputational damage, reduce fraud and comply with legal and regulatory obligations around the globe. From screening solutions through World-Check, to detailed background checks on any entity or individual through due diligence reports, and innovative identity verification and account verification – organisations can trust LSEG Risk Intelligence to help them manage their risk, so they can operate more efficiently, more effectively and more confidently. To learn more, visit www.lseg.com/risk-intelligence.

Visit lseg.com | @LSEGplc LSEG

LSEG RISK INTELLIGENCE