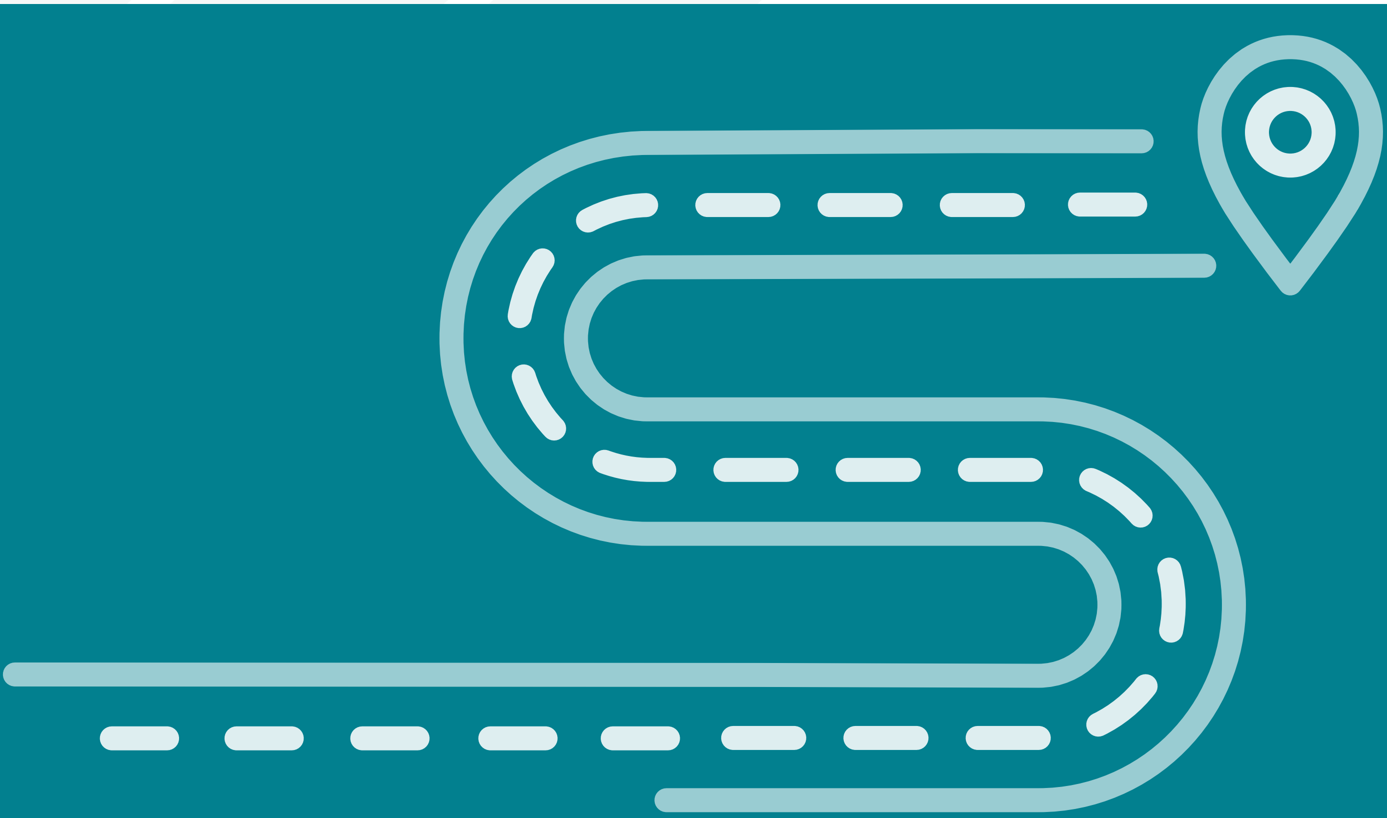
WHITE PAPER

Charting a better path for KYC:

Overcoming four key hurdles



Overview

Driving meaningful change is no small task when you're overseeing the Know Your Customer (KYC) process within your firm's anti-money laundering (AML) program.

And this challenge has only become more difficult as screening for bad actors becomes increasingly complex due to:

Aging technology that can only monitor static data at a single point in time

An overwhelming volume of data in multiple formats that are beyond human capacity to track and manage

These limitations create **inconsistencies and inefficiencies** in monitoring, which can lead to regulatory scrutiny, increased litigation costs, and frustration among compliance teams. This frustration can result in complacency – where **investigations focus more on "checking the box"** for compliance, rather than delivering meaningful, value-added insights.

Artificial intelligence (AI) is emerging as a powerful tool to enhance KYC program effectiveness.

AI-driven solutions can help deliver more consistent, accurate results when screening for bad actors. Additionally, when combined with business process automation, AI can significantly reduce inefficiencies while strengthening compliance efforts and overall program effectiveness.

However, human oversight remains essential to ensure accuracy, context, and ethical decision-making. **That's why we believe AI-assisted processes are the best path forward for institutions with KYC programs.**

While adopting AI may seem daunting, success starts with thoughtful planning – prioritizing key challenges and identifying practical solutions. To help guide you, we've outlined four critical challenges organizations face and actionable strategies to overcome them.

What's inside

CHALLENGE 1

The need for continuous monitoring

Ongoing screening for bad actors is just one part of the KYC process within AML regulations. However, as data sources and formats become more dynamic, historical methods alone may no longer be the most effective for managing a KYC program. In fact, it's estimated that **more than 80% of internet data is in an unstructured format.**

While legacy systems generate vast amounts of data, they often fail to search frequently enough or in the right places to identify potential bad actors. Not to mention, they can overwhelm teams with an excessive number of false positives, leading to inefficiencies and straining employee morale.

Understanding the world of data

	Insights	Updates	Ease of use	Format	Pool of data
20% **Structured data**	Incomplete if sole data source	Static, can be dated	Easy to store and manage	Predefined, fixed formats	Limited
80% **Unstructured data**	More insights when using LLMs	Active, in real time	Messy and complex	Multitude of formats	Abundant

Why it matters

According to **Jon Elvin**—a seasoned Certified Fraud Examiner (CFE), Certified Anti-Money Laundering Specialist (CAMS), and strategic risk advisor for Saifr—the lack of continuous monitoring is one of the most significant weaknesses in legacy technology:

"Because technologies were not historically available to do continuous monitoring without creating a significant operational impact on staff and costs, periodic monitoring became acceptable, even though it's highly risky."

"This caused the industry to accept **a risk-tiering process that is far from perfect** and can include relying on outdated technology that **only measures static data** at a single point in time and policies/programs that only flag a potential criminal once."

CASE IN POINT:

In 2024, a major U.S. bank received a consent order from the Office of the Comptroller of the Currency (OCC) to address deficiencies in its anti-money laundering practices. While no fine was imposed, the bank was required to rectify issues related to the timely filing of suspicious activity reports and correct previously identified weaknesses in its customer due diligence processes.

CHALLENGE 2

Promoting accuracy and action

Establishing a strong set of key performance indicators (KPIs) is essential for evaluating the effectiveness of any KYC program. However, several common obstacles can undermine their ability to signal potential breakdowns. Here are key challenges we've observed:

Using meaningless or outdated metrics

Many firms create broad KPIs that fail to measure the specific risks they aim to mitigate. Worse, some metrics become obsolete if they don't evolve with changing regulatory requirements.

Lack of transparency in reporting

No one likes delivering bad news, but in KYC, leadership is critical. If warning signals aren't communicated early, firms miss the opportunity to take timely corrective action.

Ignoring warning signs

A well-documented program may look solid on paper, but if KPI data signals risks (and no action is taken), its value is limited and makes the control weakness worse. Delays in addressing red flags can expose firms to significant compliance and reputational risks.

Understaffed or underqualified teams

Even the best KPIs are useless if there aren't enough skilled professionals to analyze results and respond effectively. Without adequate staffing, firms struggle to act on early risk indicators.

A strong KYC program isn't just about tracking metrics—
it's about ensuring those insights drive meaningful action.

Why it matters

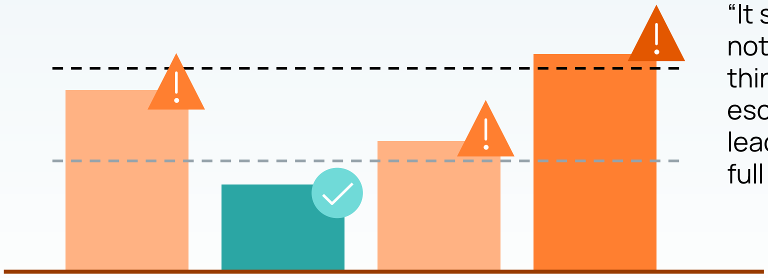
Breakdowns in a KYC program delay corrective actions, increasing the risk of compliance failures, regulatory scrutiny, and reputational damage.

While lacking metrics is a recipe for disaster, tracking too many irrelevant indicators can create a false sense of security—especially if firms rely on the wrong metrics. If your data consistently signals "green," it doesn't necessarily mean your program is effective. It may simply mean you're not measuring the right risks.

This situation was precisely the case for a major U.S. financial institution, which in 2024 agreed to pay $3.1 billion to the U.S. government over AML failures. The firm's internal reporting appeared to have failed to surface and correct issues in a timely manner.

According to Jon Elvin:

"The bank would not have passed internal audits or been operating at levels acceptable to an AML senior team if critical analysis were applied to metrics breaching yellow or red thresholds when they first emerged."



"It seems like people were not measuring the right things, issues weren't escalated properly, and leadership wasn't given full transparency."

A false sense of security can lead to a costly compliance failure—one that could be avoided with better risk monitoring, transparency, and accountability.

A healthy KYC risk management process should generate yellow and red warning signals when potential issues arise—helping to ensure that risks are identified early and can be addressed promptly. While no program can completely eliminate risk, active risk management can anticipate problems and avoid situations like the one faced by the U.S. financial institution we previously described.

Embrace the challenge: Strategies for success

Define meaningful assessment criteria

Establish KPIs that measure the actual risks your firm seeks to mitigate. One way to do this is to prioritize the quality of what you measure (e.g., the helpfulness of the information in identifying risk) over quantity (e.g., number of alerts or investigative cases). Additionally, be sure to regularly review the metrics in place and update them based on evolving regulations and real-world conditions.

Establish a corrective action process

A well-documented playbook that outlines how to respond to KPI warning signals helps ensure swift and effective intervention. Regularly review and update policies, provide ongoing training, and empower employees with the confidence to escalate concerns—knowing there's a clear plan in place for further investigation and corrective action.

Foster a culture of transparency

Encourage teams to escalate issues without hesitation—even when the news isn't favorable. Many employees fear reporting negative performance, so organizations must create a safe environment for open communication to help ensure early warning signs reach the right levels of leadership.

Ensure sufficient qualified staffing

KYC programs require skilled professionals who can interpret data, identify risks, and act on early warning signals. These teams should have the expertise to recognize operational breakdowns and adapt quickly when internal controls fail.

Rather than waiting for regulators to highlight their weaknesses, firms can make their KYC programs more trustworthy and impactful by implementing

- The right metrics
- Transparency
- The necessary tools

CHALLENGE 3

Managing risk across borders

Navigating large-scale KYC/AML initiatives across multiple countries is extraordinarily complex. Each jurisdiction has its own regulatory standards, languages, cultural nuances, and business practices—creating significant challenges in maintaining consistency. Misalignment across borders can lead to operational inefficiencies, compliance risks, and regulatory scrutiny.

For example, in **the United States**, adverse media screening is not explicitly required by law. Instead, regulators mandate that firms establish and manage a customer risk program, which may include negative media screening, but allow institutions flexibility in determining their own policies and practices, subject to applicable requirements.

Meanwhile, in the **European Union**, regulators require adverse media screening for all high-risk accounts. This regulatory inconsistency forces multinational institutions to strike a balance between meeting global standards and adapting to local requirements—often a difficult and costly task.

The challenge grows exponentially when institutions serve millions of customers and vendors across borders. Relying solely on human oversight to monitor vast amounts of data is not just inefficient—**it's virtually impossible.**

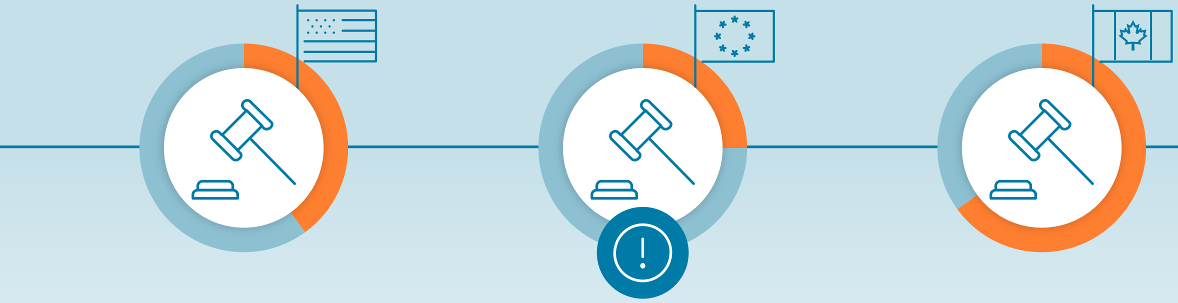
Why it matters

Inconsistent risk management

Different regulatory standards can lead to fragmented compliance efforts, particularly if firms rely on centralized teams. Imagine an institution operating in 200 countries, each with its own requirements. Managing these variations in a centralized manner is nearly insurmountable.`

Negative customer experiences

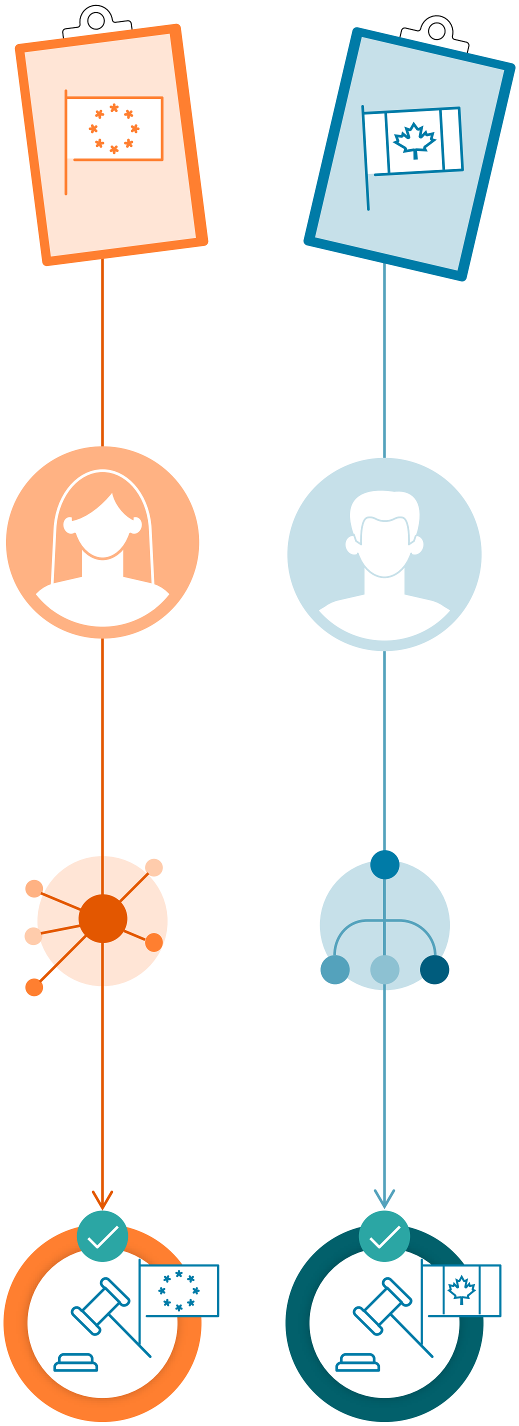
To simplify compliance, some multinational institutions have chosen to apply the most stringent regulations across all markets, regardless of local requirements. This broad-based approach—while convenient for compliance—can result in unnecessary friction and frustration for customers in countries with less rigid standards.



Regulatory blind spots

With so many moving pieces, firms may fail to recognize changes in local laws or new regulatory requirements. Without dedicated local legal monitoring, companies risk compliance lapses that can lead to fines and reputational damage.

Embrace the challenge: Strategies for success



Establish baseline standards, metrics, and workflows at the local level

Compliance must be adaptable to regional regulations. This means continuously identifying, assessing, and implementing process changes when laws shift across jurisdictions. While challenging, it's essential for maintaining operational integrity at scale.

Build strong local teams with clear responsibilities

While regulations and cultural norms differ across borders, well-trained local teams help ensure consistency in execution, provide critical on-the-ground insights, and recognize early signs of performance degradation. Compliance leaders must maintain operational line of sight and have command of the control portfolio across the ecosystem and customer portfolio.

Leverage AI while customizing it for local markets

The sheer volume of data makes manual oversight impossible. AI-powered solutions, combined with any business process automations your firm relies upon, can streamline repetitive compliance tasks, allowing human experts to focus on high-risk cases that require judgment and contextual understanding.

AI isn't a replacement for human oversight. It's an essential tool to enhance it, and leveraging AI-assisted processes is key for the foreseeable future.

Institutions can effectively and efficiently manage compliance across borders by combining

Strong governance

Localized expertise

AI-driven automation

CHALLENGE 4

Maintaining high employee engagement

Managing human capital in a KYC program presents multiple challenges. Teams often struggle with monotonous research yielding minimal results, mid-tier professionals may resist change, and employees can feel disconnected from the larger mission—especially when new technologies like AI enter the picture.

Fear is a major factor in this resistance. It can often stem from a lack of employee confidence, training, and skills needed to embrace something new, as well as concerns over job security.

Without the right mindset, leadership, and tools, firms risk:

Losing engagement

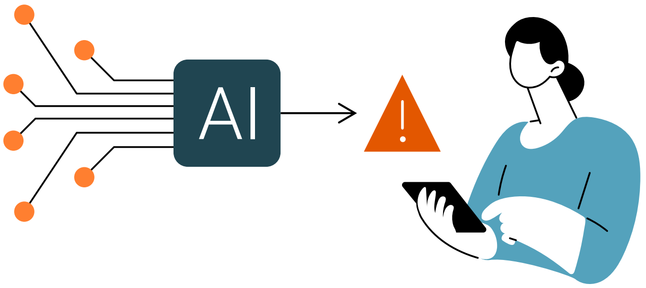
Lowering morale

Undermining the effectiveness of KYC programs

Why it matters

Employee experience is critical to the success of any KYC/AML program. The more effectively AI is integrated, the less time employees spend on repetitive, low-value tasks—reducing unnecessary client interactions while enhancing privacy and security.

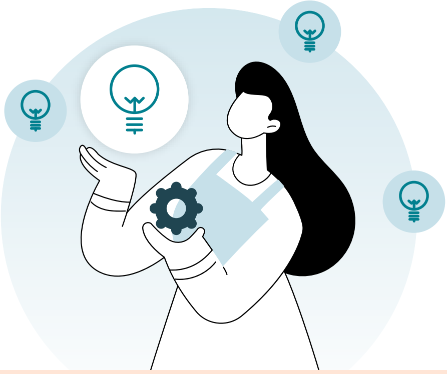
When teams focus on the right risk indicators instead of sifting through 90%+ false positives, morale improves, engagement increases, and the overall employee experience is elevated.



Without AI, employees could waste valuable time documenting legitimate customers instead of identifying actual bad actors.

Leadership also plays a pivotal role in shaping engagement.
If leaders fail to inspire and support their teams, the entire program suffers. A Chief Risk Officer, for example, must demonstrate intent, vision, and leadership to foster a high-performing, committed team. Without this, the program risks becoming a check-the-box exercise, leading to mediocrity at best.

High-performing teams are driven by purpose, curiosity, and a willingness to explore new possibilities.



In contrast, employees who feel unsupported, uninspired, or left in the dark tend to resist change, avoid risks, and settle for routine. The difference between merely keeping up and achieving breakthrough success often lies in an organization's ability to nurture an experimental, forward-thinking mindset.

Embrace the challenge: Strategies for success

Foster a mindset of possibility

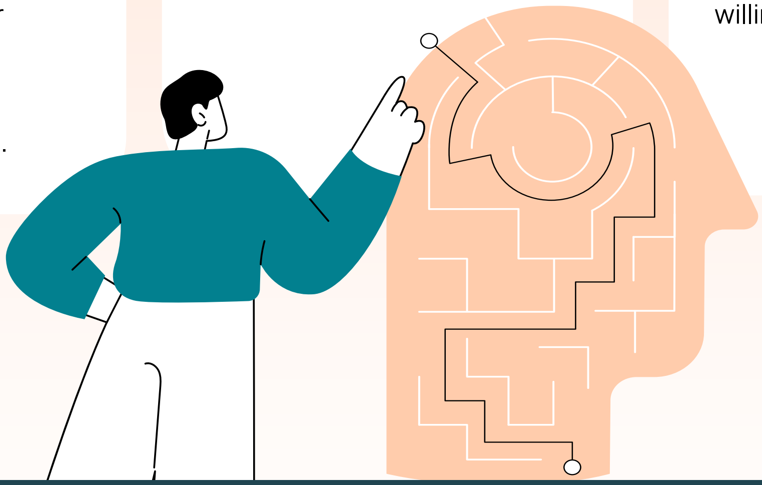
Instead of focusing on what could go wrong, encourage teams to explore what could go right. Experimentation doesn't mean blindly overhauling systems—it means being open to new ways of improving processes, efficiency, and customer experience. A culture of innovation and inspiration drives better engagement and results.

Be intentional in hiring and leadership development

Leadership matters at every level. Prioritize hiring leaders and managers who not only bring the right skills but also have the ability to motivate, mentor, and inspire their teams.

Prioritize the employee experience

Educate and inspire your workforce. When employees see the bigger picture—how their work protects customers, strengthens the brand, and upholds compliance—they become more engaged, invested, and willing to embrace change.



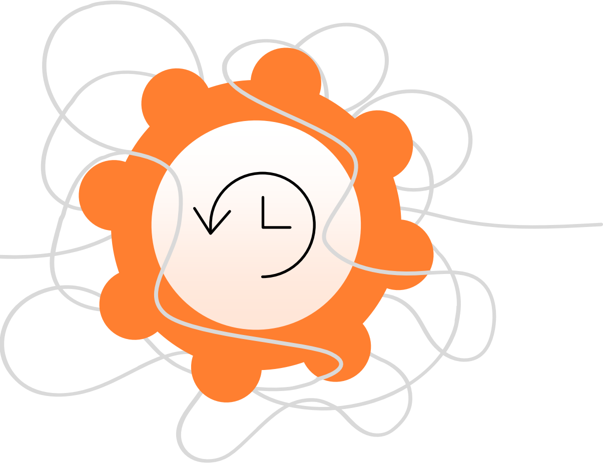
Organizations can build stronger and more engaged teams that drive greater KYC/AML success by fostering a culture of

Innovation

Empowerment

Leadership

Conclusion



The evolving landscape of financial crime and regulatory scrutiny demands a more proactive, technology-driven approach to KYC compliance. Traditional methods, constrained by aging technology, data overload, and inconsistent monitoring, are no longer sufficient to meet today's challenges.

Institutions that fail to embrace a proactive, technology-driven approach face three risks:

- **Inefficiencies**
- **Compliance failures**
- **Reputational damage**

AI-powered solutions, combined with human expertise, present the strongest path forward.

By leveraging AI for continuous monitoring, data screening, and review, firms can

- ✓ **Enhance accuracy**
- ✓ **Reduce false positives**
- ✓ **Free up teams to focus on high-value investigations**

However, success doesn't come from technology alone—it requires

- ✓ **Leadership commitment**
- ✓ **Cultural transformation**
- ✓ **A willingness to embrace innovation**

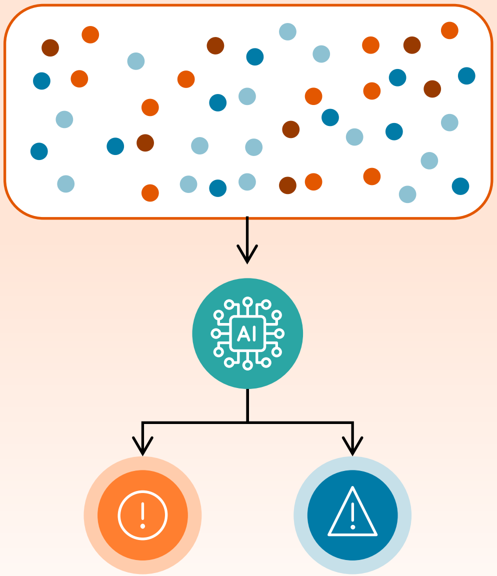
The four challenges outlined in this brief represent key hurdles that every organization must overcome.

By addressing these issues head-on and strategically integrating AI-assisted processes, firms can build stronger, more efficient, and resilient KYC programs.

About SaifrScreen^{SM}

SaifrScreen^{SM} enables firms to more accurately and efficiently review continuously for potential risks in full customer and vendor populations. It leverages the latest in machine learning (ML) technology and natural language processing (NLP), including large language models (LLMs).

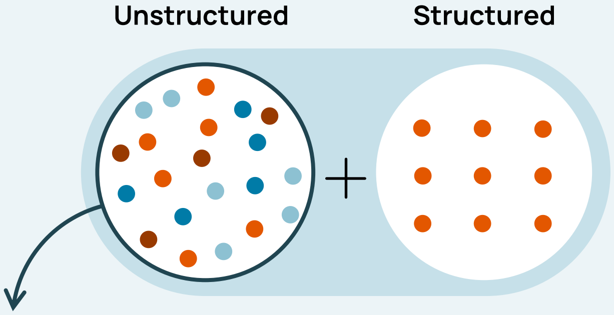
SaifrScreen is uniquely able to review large populations against publicly available information to identify potential indications of financial or reputational risk.



SaifrScreen uses behavioral science to understand context and can distinguish media that describes fraud versus murder, for example. Additionally, SaifrScreen crawls and indexes internet data 24/7 to provide ongoing review and monitoring with early warning notifications. These potential risks can feed into firms' processes for further investigation.

SaifrScreen's data advantage helps clients find more potential risks, sooner.

Most traditional AML and KYC screening and monitoring methods focus solely on structured data (e.g., sanctions, wanted, and watch lists), which **only represents ~20% of internet data** and can be **slow to be updated.**



SaifrScreen extends its reach to unstructured data, including:

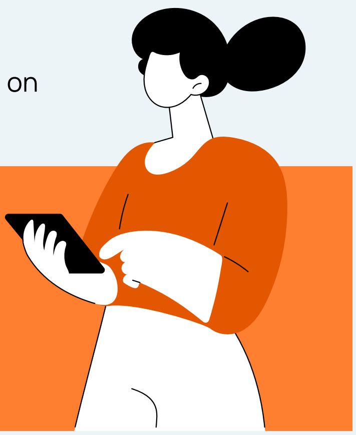
230K	190	160	23B	millions
sources	countries	languages	webpages	of data added daily

Subject to change

SaifrScreen's continuously growing dataset includes sources such as news media, government sources, arrest and court record aggregators, and more. Searching this remaining ~80% of internet data can reveal valuable details and enables firms to zero in on and further investigate potential threats, such as fraud, as soon as they are flagged.

Up to **7x**
as many potential bad actors identified

Compliance officers using SaifrScreen are empowered to address more cases without sacrificing hours chasing dead ends via menial, manual methods.



saifr

About Saifr

Saifr, a RegTech within Fidelity Investments' innovation incubator, Fidelity Labs, is committed to safeguarding organizations from pervasive AI and regulatory risks. Using intelligent technology that efficiently and effectively navigates complex compliance and regulatory requirements, Saifr helps clients save time, reduce costs, and improve accuracy while protecting the firm. Our advanced, AI-powered risk mitigation and management solutions include capabilities for marketing compliance review, adverse media review and monitoring, and electronic communications surveillance.

Saifr's products and services include tools to help users identify potential leads for further investigation. Saifr is not a consumer reporting agency as defined under the Fair Credit Reporting Act (FCRA), and its products and services may not be used to serve as a factor in establishing an individual's eligibility for credit, insurance, employment, benefit, tenancy, or any other permissible purpose under the FCRA. Saifr's products and services are not intended to replace the user's legal, compliance, business, or other functions, or to satisfy any legal or regulatory obligations. All compliance responsibilities remain solely those of the user.