saifr®

WHITE PAPER

Mitigating risk in the digital age:

A roadmap to AI-enhanced adverse media screening

Overview

If you're responsible for adverse media screening within your organization, it likely comes as no surprise that efforts in this area are often incomplete.

The harsh reality is that long-standing estimates measure money laundering at 3-5% of global GDP. What's more, in 2023 one US financial institution was fined $4 billion for violations involving anti-money laundering (AML) actions. With such staggering figures, it's no wonder **risk management professionals are challenged with optimizing their screening processes** to protect their organizations, their customers, and themselves.

While ongoing screening for bad actors is just one component of the Know Your Customer (KYC) process within AML regulations, it's an important one. **Technology has long played a role in adverse media screening**, with traditional offerings built on core matching technologies designed to read lists of structured data from a multitude of registries. While these offerings can produce lots of data, they often fail to search frequently enough or in the right places. Not to mention, traditional tools can yield an unmanageable number of false positives, which can hamper your team's organizational efficiency and morale.

Artificial intelligence (AI) provides a new path forward. AI-based tools are intended to strengthen a firm's AML/KYC risk and compliance program by screening for bad actors with greater precision and efficiency than traditional offerings. **They're not intended to replace humans dedicated to screening and investigating potential bad actors.** Instead, they are technology-assisted tools designed to help make your team stronger and smarter, improving the performance of your risk management program.

We created this white paper to help you thoughtfully embark on an evaluation of the potential options for AI-based adverse media screening tools.

It's organized across five key considerations to help you start your search with the right questions.

What's inside

CONSIDERATION #1

Choosing advanced screening or adopting a full-AI solution

It seems like most vendors offer some type of AI, so it's important to first understand what type of solution you're evaluating:

Traditional list-based screening and monitoring that may have AI-like capabilities

or

AI-enhanced screening and monitoring that does far more than matching for keywords

Knowing the difference can help you avoid solutions that provide no advantage over technologies you're already using.

Types of AI that may be used in adverse media screening tools

SIMPLE

Rules-based tools alert you whenever designated keywords appear, regardless of context. They generate matches to a query by using a library of language rules. Thus, they can produce large amounts of results that need human evaluation as well as more false positives. For example, monitoring for "impersonator" may return results that include comedians and actors. Ultimately, such rules-based AI may not be as effective or efficient as desired.

Machine learning (ML) enables computers to recognize complex patterns without humans describing the patterns of interest. The machine isn't just taught: it actually learns.

Once trained, ML models can handle new scenarios and understand context. So, in the "impersonator" example, an ML model would be less likely to flag comedians or actors. Traditional rules-based solutions may incorporate ML to offer advanced screening capabilities. For such solutions, it's critical to understand the data types the solution relies upon. Learn more about data sources in the next section.

Generative AI is a type of deep learning within the realm of machine learning. As its name suggests, it can generate text, images, software code, music, and videos, and even problem solve. In text generation, the AI predicts—and produces—the next most likely word in a sequence.

Large language models (LLMs) are a type of generative AI—deep learning algorithms equipped to summarize, translate, and predict text. LLMs rely on massive datasets, which may include >100 million parameters.

LLMs can read text like a human, which allows these models to identify a bad actor within the context of an article. As such, LLM solutions can be one of the best ways to discover more bad actors earlier, lowering overall risk with better efficiency.

Using LLMs lets you tap into data on more potential bad actors and find them earlier

COMPLEX

THE BOTTOM LINE

ML solutions offer the greatest potential to improve screening for potential bad actors. However, it's important to dig deeper into any AI option to understand whether it's just enhanced core matching or uses a full-fledged LLM.

Starter question

? Is the solution a traditional list-based screening that may have AI-like capabilities, or an AI-enhanced screening that offers more than keyword matching?

CONSIDERATION #2

Sources and types of data used

Let's face it: we operate in a data-driven society where businesses rely on data analytics to make informed decisions and gain a competitive advantage. While it's natural to focus on the amount of data a solution taps into, we feel **the better approach is to focus on data sources and types**. As we mentioned earlier, not all AI solutions can tap into all types of data.

Data comes in two formats: structured or unstructured. More than 80% of the world's available data is unstructured, yet most traditional core matching technologies only read structured data. Relying on traditional technology means you're only screening 20% of available data.

20% Structured data

These data are found in a predefined format in curated databases, such as politically exposed persons lists, sanctions lists, and internal watch lists. They're considered static data, meaning they have to be manually updated.

Structured data are easy to store, organize, and use. Yet, they represent a very limited pool of the world's data and are only captured at a single point in time. As result, they can still lead to incomplete results and greater risk.

80% Unstructured data

These are active, real-time data that take many forms, including multimedia files, emails, videos, text messages, audio, and web logs, which are harder to search and use. These types may feel messy because they lack any predefined format—yet can provide a wealth of information.

However, the massive quantity of unstructured data means that no amount of people could ever sift through it all. Imagine trying to read the entire internet! One of the best ways to tap into unstructured data is with LLM technology. By pointing your screening engine at a larger corpus of data effectively and efficiently, you can identify more risk in absolute terms.

Unstructured data have the potential to deliver countless insights to make more informed decisions

Limited pool of data ✗	✓ Abundance of data
Predefined fixed format, often from prepopulated lists ✗	✓ Multitude of formats, including videos, chats, images, emails, social media, business or legal documents
Easy to store and manage ✓	✗ Messy
Static, can be dated ✗	✓ Active, real-time
Incomplete insights if sole data source ✗	✓ Efficiently surfaces more insights when using LLMs

THE BOTTOM LINE

AML/KYC risk management solutions that rely on structured data are missing out on 80% of the world's available data. Meanwhile, solutions that surface results from unstructured sources can help identify more potential criminals because they monitor real-time data.

Starter questions

- ? Does the solution rely on structured or unstructured data?
- ? If unstructured data are used, what's the population size and scope?
- ? Can unstructured and structured data sources be integrated together in a search?

CONSIDERATION #3

Essential features

The next step for a potential new system is considering how to use it to your maximum advantage. Since not all firms have the same needs, we encourage you to explore **how specific features of any new solution align with your goals**. Here are a few that can improve screening precision and efficiency:

Screening based on specific criminal typologies and risk tolerances
For example, a client could request to see only financial crimes if crime proceeds may be on their platform.

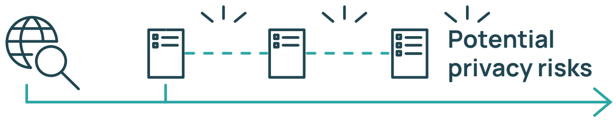
Ability to upload your firm's own data
Most firms likely have stored unstructured or proprietary data that could be leveraged. Integrating such data can help you fine-tune the relevance of the results surfaced.

Entity resolution
Associating unstructured data with an actual entity is key to efficient screening. For example, the system could determine that web documents about someone involved in a crime are likely about an entity being screened.

Maintain privacy by gaining more control of the data

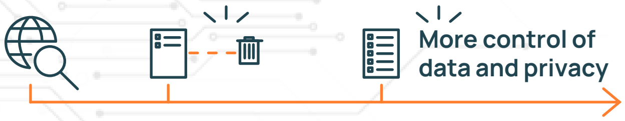
There are real privacy concerns about traditional technologies storing dossiers on potential bad actors. Tools that screen unstructured data sources can help. Specifically, LLM-based tools conduct real-time searches of frequently enriched data, and you can maintain or discard the results based on your analysis. Future searches can then be conducted anytime with fresh data, putting the user in control.

Traditional tech approach



- ✓ Government sites are canvassed for stories about ABC, a potential bad actor
- ✓ Dossier is created and maintained in a database, without regard for whether ABC has been verified as a good or bad actor
- ✓ Information is added to the stored dossier over time until the situation is resolved

Machine learning approach



- ✓ Models search for active data about ABC
- ✓ Real-time results about ABC are surfaced, e.g., the correct articles
- ✓ Results are saved or discarded based on your team's analysis
- ✓ Even if results are discarded, you can search a new pool of active data in the future

THE BOTTOM LINE

Customization features can make your screening process even more precise and efficient. By assessing these features against your firm's needs, you can select the best possible tool to align with your objectives.

Starter questions

- ? What are my needs for customization? How will this evolve over time?
- ? Which features find more bad actors with greater precision and efficiency?
- ? How does entity resolution work?
- ? What are the specific ways privacy is protected?

CONSIDERATION #4

Claims about false positive reductions

Investigating false positives is tedious, requiring an extensive amount of your team's time. Not to mention, **the more false positives a solution generates, the fewer real risks your team is surfacing**. With many vendors making claims about reduced false positives, how do you go about verifying their statements?

Here are two steps to take when presented with such claims:

1 Understand the type of technology used and its feature set

As we've established, you need to understand a system in order to tailor it to your needs. Knowing what type of AI a solution offers is important, as that drives the type of data it can access.

Further, the feature set influences the accuracy in identifying bad actors. Features like entity resolution can significantly **reduce false positives with earlier and better matching**. What's more, **minimizing false negatives can save on costly regulatory fines**.

2 Ask for proof of false positive claims

Once you understand the technology type and feature set, you should seek proof of the claims made. Whether the vendor claims reductions of 30% or 80% in false positives, we believe it's difficult to determine the value of a platform without a basis for comparison. Probing for proof of claims can take several forms:

Results from any head-to-head matchups

Comparing the technology against other systems can help you see whether the matchups find more bad actors with significantly fewer alerts. For example, finding double the number with half the alerts means 50% more bad actors surfaced that you wouldn't have known about.

Case studies of happy customers

These studies should document before and after states and include actionable data that support finding more bad actors with fewer alerts.

Asking for references

Other risk managers may be happy to share their candid experiences. For such conversations, ask for specifics regarding improvements in false positives, along with whether more bad actors were surfaced. Try to contact at least three references.

Seek and evaluate multiple forms of proof for vendor claims about improvements in false positives.

THE BOTTOM LINE

Advanced technology doesn't have to be an unknown risk. While false positives are inevitable, you can gain more confidence in a potential solution's capabilities by understanding what makes the technology work and asking for proof.

Starter questions

- What is the basis for claims of reductions in false positives?
- Is there specific proof, like results from a head-to-head or case studies?
- Can you introduce me to three references who are using your solution?

CONSIDERATION #5

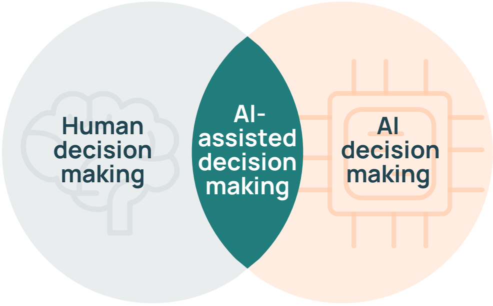
Organizational opportunities

As part of the screening process, we encourage you to consider how an AI solution can enhance your team's value as well as how to take a responsible approach in adopting this new technology.

Enhance the value of your team

It's only natural to consider the impact on your staff, who have been tediously performing manual screenings. Our view is that an AI solution can enable greater job satisfaction and professional growth. Why? Because your team can be trained on higher-level investigative activities, **a shift from confirming your screening system's scoring to more in-depth evidence gathering**.

Investigation is a manual process, as it requires judgment calls. Technology cannot replace that, though it can automate cumbersome tasks like sorting through millions of data points. Because decision-making is a human function, the key to a strong risk and compliance program isn't decision-making technology—it's **technology-assisted decision-making**. Whether you operate an AML program or manage third-party risk, investigation should always have a human in the loop.



Embrace responsible innovation

We believe that regulators generally encourage innovation and support the thoughtful exploration of AI. Below are some ideas you may want to consider as part of your approach to embracing innovation responsibly:

Conduct regular risk assessments

These should include a range of outcomes, from what can go well to what can go wrong.

Such assessments build internal confidence in new technology and confidence with regulators.

Run a study

Why not run your existing system in parallel with a new AI-based solution for six months?

Monitoring the results can help you gain assurance and demonstrate a responsible approach.

Create a risk management plan

Regulators will want to know how you monitor the risk of a new system. This includes reviewing the output against hypotheses, creating key risk indicators and safeguards, and documenting the steps you'd take in case of a system failure.

THE BOTTOM LINE

Adopting any new technology means change. When exploring AI, don't overlook opportunities to enhance the employee experience and overall value of your team. A thoughtful and responsible approach to innovation can encourage confidence in your organization and the regulatory bodies that oversee it.

Starter questions

- What can you gain by elevating team members from manual screening tasks to investigative responsibilities?
- How and how often will you monitor a risk management plan?
- What key indicators will act as warning signals for scenarios that could go wrong?

Track your findings

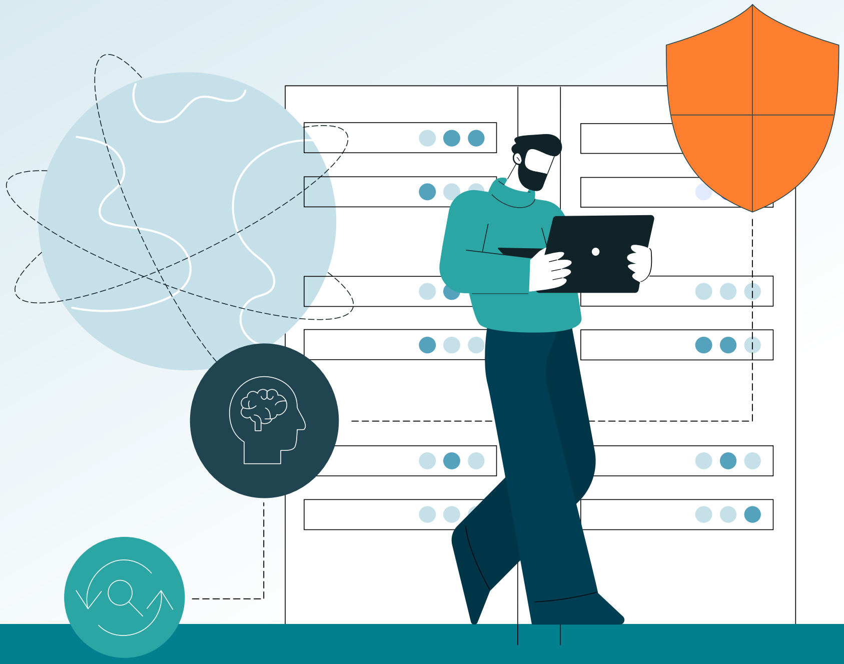
As we presented in this white paper, AI-based screening tools can lead to better outcomes by **strengthening your risk and compliance program with greater precision and efficiency** than traditional offerings. What's more, adopting such tools can improve the employee experience while strengthening your team in the process.

As you thoughtfully embark on an evaluation of the potential options for AI-based screening tools, you may want to use the following template to help start your search with the right questions.

	Sample questions	Did the response meet my needs?			Notes
		Yes	No	Needs further investigation	
CONSIDERATION #1 **Advanced screening or adopting a full-AI solution**	Is the solution a traditional list-based screening that may have AI-like capabilities, or an AI-enhanced screening that offers more than keyword matching?	○	○	○	
CONSIDERATION #2 **Sources and types of data used**	Does the solution rely on structured or unstructured data?	○	○	○	
	If unstructured data are used, what's the population size and scope?	○	○	○	
	Can unstructured and structured data sources be integrated together in a search?	○	○	○	
CONSIDERATION #3 **Essential features**	What are my needs for customization? How will this evolve over time?	○	○	○	
	Which features find more bad actors with greater precision and efficiency?	○	○	○	
	How does entity resolution work?	○	○	○	
	What are the specific ways privacy is protected?	○	○	○	
CONSIDERATION #4 **Claims about false positive reductions**	What is the basis for claims of reductions in false positives?	○	○	○	
	Is there specific proof, like results from a head-to-head or case studies?	○	○	○	
	Can you introduce me to three references who are using your solution?	○	○	○	
CONSIDERATION #5 **Organizational opportunities**	What can you gain by elevating team members from manual screening tasks to investigative responsibilities?	○	○	○	
	How and how often will you monitor a risk management plan?	○	○	○	
	What key indicators will act as warning signals for scenarios that could go wrong?	○	○	○	

Save time and strengthen AML/KYC programs with SaifrScreen℠

SaifrScreen enables firms to **more accurately and efficiently screen** continuously for potential risks in full customer and vendor populations.



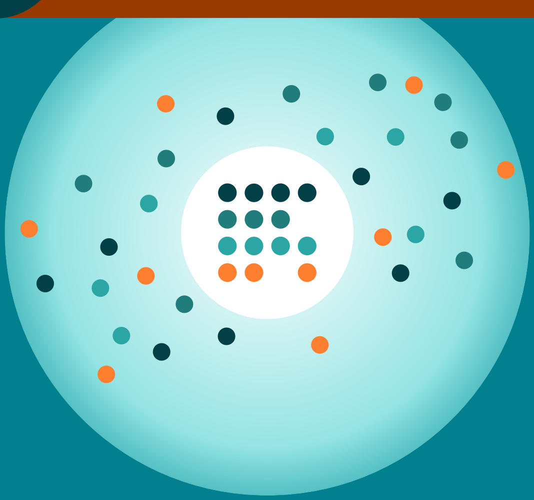
Using the latest in machine learning technology and natural language processing (NLP), including large language models (LLMs), SaifrScreen is uniquely able to screen large populations against publicly available information to identify indications of financial or reputational risk and resolve them to either a person or a company.

SaifrScreen also uses behavioral science techniques to understand context and can distinguish behaviors that indicate fraud versus murder, for example. Not to mention, SaifrScreen crawls and indexes data 24/7 to provide ongoing screening and monitoring with early warning notifications.

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 (such as sanctions, wanted, and watch lists), which represent only 20% of internet data and can be slow to be updated. **SaifrScreen extends its reach to unstructured data**, including 230K sources from 190 countries in 160 languages.

With 23 billion webpages indexed, and millions more added daily, the continuously growing dataset includes sources such as news, social media, government sources, arrest records, and more. Searching the remaining 80% of internet data reveals actionable details and enables firms to identify threats, such as fraud, as soon as they become known.

With **23 billion webpages indexed,** SaifrScreen monitors both unstructured and structured data



47% FEWER FALSE POSITIVES SURFACED

7X THE NUMBER OF BAD ACTORS IDENTIFIED

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

saifr.ai/saifrscreen

Client improvement experiences are for representative purposes only. Results may vary based on different factors unique to a financial institution and its customer base.

saifr®

About Saifr

Saifr®, a RegTech within Fidelity Investment's 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 prevention and management solutions include capabilities for marketing compliance review and adverse media screening and monitoring. Learn more at https://saifr.ai.

Please note that all compliance responsibilities remain solely those of the end user(s) and that certain communications may require review and approval by properly licensed individuals. Fidelity is not responsible for determining compliance with rules and will not be liable for actions taken or not taken based on Saifr's products and services.