rdc
Smarter Screening

FIVE STEPS FOR BEST-IN-CLASS CUSTOMER SCREENING

PROVEN TECHNIQUES FOR BETTER SCREENING

Today, due diligence is more important than ever. Screening and monitoring is essential – not only for compliance with complex regulations, but also to protect your organization against genuine business and reputational risk. Due Diligence can be time-consuming and costly to get right. Getting it wrong? That’s even costlier.

In this eBook, we present proven steps to create a customer screening program that protects your business while keeping your costs under control.

1. Concentrate on data quality
2. Don’t rely on search engines
3. Look beyond sanctions
4. Take care of the post onboarding stage
5. Keep an eye on scale and cost

1. CONCENTRATE ON DATA QUALITY

Customer due diligence is all about answering two fundamental questions:

> **"Are you who you say you are"?**
>
> **"What level of risk do you present to my organization"?**

Clean customer records
The answers to these questions start with your customer data. If it's incomplete or inaccurate, this can lead to poor name matching and high rates of 'false positive' results. In our experience, few companies invest enough in cleansing their data. Yet it is possible to improve screening results by at least 50% just by adding accurate date of birth and location information to a standard first name/last name record.

Trusted, curated screening data
However, simply adding more data is not always the answer. Especially if you're screening for adverse media, for example, where more does not always mean better. For adverse media, it's particularly important to follow some best practices:

- **Trusted sources.** Make sure adverse media screening covers credible, trusted sources that follow journalistic best-practice – and that it doesn't include "fake news".
- **Global coverage.** If adverse media screening only covers national sources it may miss out on important stories from elsewhere in the world, so it's important to cast your net as widely as possible.
- **Indexed and curated data.** When adverse media data is well indexed, it can give you a much more accurate and complete picture, for example:
  - Location and related individuals
  - Types of risk or crime, e.g. abuse, bribery, money laundering
  - Different risk stages, e.g. accused, arrested, convicted

In summary – make sure you screen against data that is up to date, from reputable sources and curated for easy retrieval and filtering.

"It is critical to have complete and high-quality static data, which is the raw material used for risk rating and related mitigating controls."

"Reliable AML controls based on complete and accurate static data; An ongoing challenge for professionals", Deloitte

2. DON'T RELY ON SEARCH ENGINES

Internet search is fast and free, which is why many companies employ compliance analysts to screen prospects and partners using well-known search engines. Yet while they are quick and easy to use, search engines are poor due diligence platforms, for four good reasons:

The problems with internet search

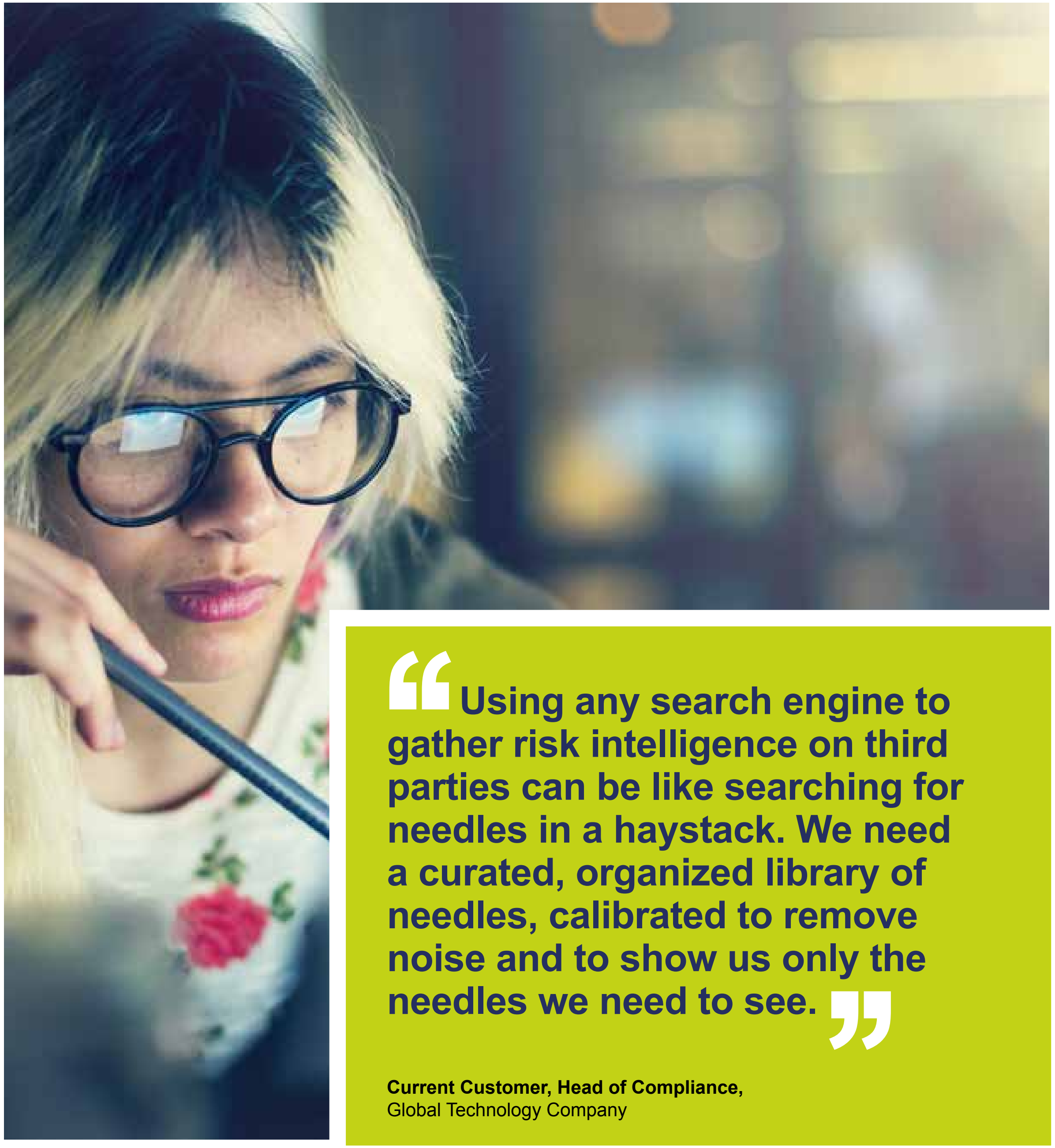
1. Results vary dramatically depending on factors such as user location, user profile, search history and time of day
2. There's no track record or audit trail
3. It's difficult to filter results based on risk policy, customer segmentation, etc.
4. Irrelevant results lead to false-positive rates of 95% or higher

Speed and accuracy: the power of a purpose-built platform
For due diligence, a purpose-built screening platform can overcome all of the limitations of internet search, leading to faster and more accurate results:

Name-matching technology based on machine learning and natural language processing means your searches produce fewer alerts and false positives
With a full history of screening data and outcomes, you can optimize filters to get maximum coverage with the least amount of alerts
Comprehensive and accurate sanctions, watch list and PEPs data means you can be confident your searches are not missing anything

The power of SaaS
Easy to roll out and use, Software-as-a-Service (SaaS) architecture has a number of advantages that make it the ideal foundation for a due diligence platform that protects your organization:

Up-to-date. You always have access to the most current watchlists and data sources
Scalable. Rollout across the organization is fast and easy, regardless of how many users need access
Secure. A good SaaS due diligence platform offers the highest levels of security
Low cost of ownership. With no maintenance or installation costs, it's the cost effective way to deploy due diligence capability



> **"Using any search engine to gather risk intelligence on third parties can be like searching for needles in a haystack. We need a curated, organized library of needles, calibrated to remove noise and to show us only the needles we need to see."**
>
> **Current Customer, Head of Compliance,**
> Global Technology Company

3. LOOK BEYOND SANCTIONS

Nearly all organizations screen prospective customers and partners against government-issued watchlists such as the US Treasury's Office of Foreign Assets Control (OFAC) list.

Well documented and publicly available, these lists are designed to restrict commerce with targeted foreign countries and regimes, terrorists, narcotics traffickers, people engaged in activities related to weapons of mass destruction and other threats to national security.

The importance of Politically Exposed Persons (PEPs)
For many, this is the extent of their compliance screening program – and alone, it can be time-consuming. However, restricting compliance activity to sanctions lists misses risks associated with PEPs.

"63% said sanctions compliance has consumed more time, money and personnel in the past three years, with the biggest cause being the growing complexity of the task due to more information available and longer lists."

Deloitte, February 2018
"Facing the Sanctions Challenge in Financial Services"

Risk-based screening
If a potential partner or customer is in a position of power or influence (or may be related to or associated with someone who is), they may present a higher risk. The level of risk depends on factors such as their role, their level and their country. If you take a risk-based approach to PEP screening however, it's possible to maximize protection without creating excessive extra work or generating false positives.

Examples of PEPs
- Heads of state and cabinet officials
- Ambassadors and top diplomatic officials
- Senior military figures
- Senior judicial figures
- Political party figures
- Top functionaries in state-controlled businesses, their family members, close associates and advisors

Add adverse media
While it's essential to screen against both sanctions and PEPs, a Know Your Customer (KYC)/ anti-money laundering (AML) program is incomplete unless it also covers adverse media. This refers to references about individuals across a wide range of published sources. Prior to being added to the OFAC list, many entities are in the news for risk- related crimes. This information can help you avoid risk, for example by revealing that potential customers or partners are involved in bribery & corruption, drug trafficking and money-laundering — all of which would cause serious commercial and compliance issues.

Adverse media checklist
To be effective, an adverse media source should have five characteristics:

- **Profile-based.** Easy to relate to individuals, and not just a list of news stories
- **Risk relevant.** Not all data about "John Doe" is relevant to compliance, so data sources should focus on risk-relevant content
- **Coverage.** Content should be global in nature and include both printed and digital media
- **Credible.** Adverse media references should come only from reliable and trusted sources
- **Current.** There should be clear process for updating content

"A defined adverse media screening policy can help banks better mitigate risk and make more informed decisions about customers."

AML & KYC: Adverse Media Screening and the Data Challenge
Accenture, November 2017

4. KEEP MONITORING POST-ONBOARDING

Due diligence doesn't end when business relationships begin. The simple reason is that circumstances change. Any customer or partner could become involved in activities that clash with compliance, putting your organization at risk.

Many organizations screen either once a year or take a segmentation approach, only re-screening the highest-risk customers. However both these methods can leave you exposed, as the table below summarizes:

Problems with post-onboarding approaches

Annual re-screening	Segmentation
• Labor-intensive • Expensive • Leaves organization exposed between onboarding and re-screening	• High-risk individuals are difficult to identify • Remaining customers or partners may also expose you to risk

Continuous protection
The ideal post-onboarding compliance model screens your business relationship on a continuous basis, with two key features:

- Automated daily portfolio monitoring
- Lists and adverse media that are updated daily

Systems that achieve this typically do so using by applying advanced machine learning and natural language processing to high-quality sources of risk intelligence.

"58% of respondents uncovered legal, ethical or compliance issues with a third party after initial due diligence."

Anti-Bribery and Corruption Benchmarking Report, Kroll/Ethisphere, February 2018

"Implementing overnight screening has not only saved us time by replacing certain elements of our manual screening but it has also enabled us to manage risk in a more comprehensive and proactive way."

Current Customer, Head of Compliance,
Major European Investment Firm

5. CONTROL SCALE AND COST

Even if they have the best possible set-up for KYC/AML screening, many organizations struggle with the cost of compliance, both from a financial and operational efficiency perspective. Some of the most common causes are outlined below, alongside potential remedies.

Problem	Solution
High alert rates and false positives Many companies still employ large teams of Level 1 and 2 analysts to manually filter the alerts for the records that matter. This can lead to high costs and slower onboarding.	• Improved customer data • Advanced name-matching technology • Better screening data
Distributed compliance operating model In most organizations, regions or business units use different definitions of risk and materiality, or different screening processes. The lack of a consistent global standard can lead to redundant processes, excessive headcount and longer, costlier audits.	"Center of excellence" model: • Ensures global consistency • Digitizes costly processes • Reduces matching workload • Cuts alert processing time
Delay in AI adoption With 2.5 exabytes of information produced every day, human-based searching is rapidly becoming irrelevant for complex, business-critical tasks like compliance screening.	Benefits of AI include: • Eliminating repetitive work • Freeing staff for higher-value work • Improving efficiency • Performing calculations impossible for humans

"False positives were reduced by 50-75% and the time needed to clear the remaining alerts decreased 30-50%."

Current Customer, VP - Head of Compliance,
Global Financial Advisory and Asset Management Firm.

"The first challenge is for the bank steering function to become more efficient. Methods for doing so include adjusting the organizational setup and operating model and optimizing the powerful potential of new technologies."

Global Risk 2017: Staying the Course in Banking,
Boston Consulting, Group, March 2017

"AI will over time provide a better experience for customers and employees while delivering real business value on every dimension."

Artificial Intelligence in Banking, Celent Research, August 2017

BEST-IN-CLASS CUSTOMER SCREENING

Six actions to take now

- **Invest in data cleansing** to improve name-matching and reduce false positives
- **Augment Level 1 Analysis** with a purpose-built screening platform
- **Screen against sanctions, watchlists, PEPs and adverse media** to maximize protection and compliance
- **Use continuous portfolio monitoring** to eliminate blind spots in your customer base
- **Consider a center-of-excellence (COE) model** for further efficiency and savings
- **Leverage AI** to dramatically reduce alert rates and costs while improving response times