Using AI to Support Public Searches in KYC

Force for good.

www.idenfo.com

Author

Antony Bellingall

Co-Founder, Idenfo

The Cost of Compliance

Name Screening and
Public Information Checks

The challenge with Public Searches

Automating with the assistance of AI
– introducing Intelligent Search

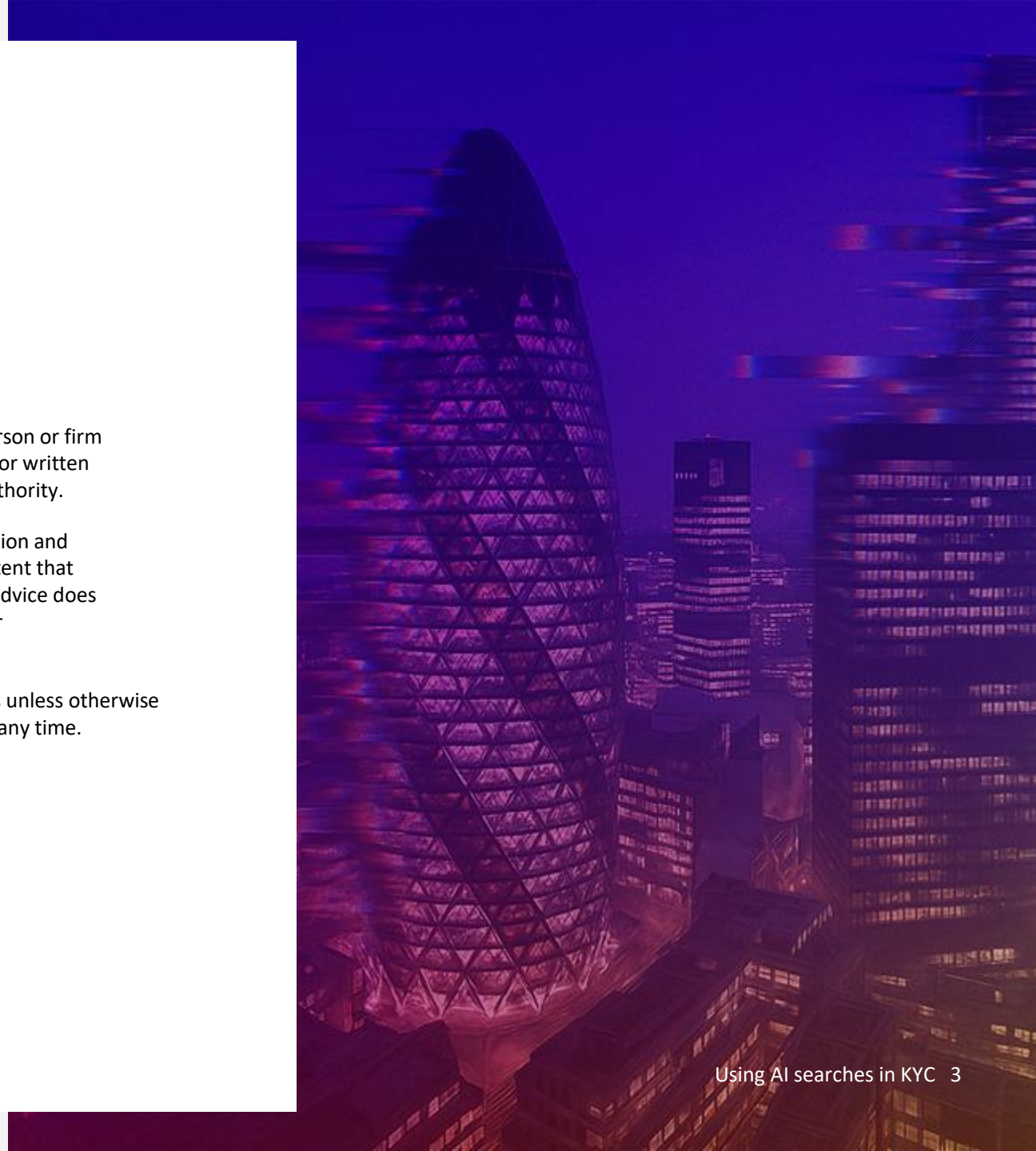
Legal Statement

This document contains proprietary information belonging to Idenfo Ltd.

No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the express prior written permission of Idenfo Ltd, excepting a demand by an appropriate Regulatory authority.

The text, graphics and examples included herein are for the purpose of illustration and reference only. No legal or accounting advice is provided hereunder. To the extent that this document provides suggestions for efficient compliance processing, such advice does not constitute legal advice and in no way assumes on Idenfo a responsibility for compliance obligations.

Corporate and individual names and data used in examples herein are fictitious unless otherwise noted. Idenfo reserves the right to revise this document or any part thereof at any time.



Executive Summary

There is a material cost of AML compliance: UK banks spent approximately £34.5 billion annually on AML compliance in 2023 and these costs are rising fast.

The average corporate account setup costs for performing KYC comes to £230. A significant portion (28% or £63) of this is attributable to public internet searches, especially reviewing adverse media and conducting supplementary PEP checks.

The main databases used for screening are sanction, PEP and special interest lists. Public searches supplement database checks to address their limitations, notably in identifying newly appointed or lesser-known PEPs and recent adverse media.

Public search procedures are labour-intensive and error-prone—agents must investigate, validate, compile, and review evidence for each client, particularly around negative news or PEP status.

AI-based solutions, such as those developed by Idenfo, can automate much of the KYC research and assessment, generating consistent, evidence-based, and rapid decisions on PEP/adverse media status.

The Idenfo Intelligent search tool provides:

- A true/false determination for PEP and adverse media hits.
- A one-line evidence summary and detailed bullet points for all findings.
- Numbered URLs linking directly to each piece of supporting evidence for efficient human review.
- A consolidated view for compliance teams, speeding up checks and improving accuracy.

Moving to AI based solutions confer a number of advantages for regulated institutions:

- AI automates routine checks, allowing human compliance agents to focus on high-risk or complex cases.
- It is capable of ongoing, real-time monitoring and risk scoring, adapting swiftly to regulatory changes or evolving client risk profiles.
- It dramatically reduced the volume of false positive alerts and so improves overall compliance operational efficiency.
- It is supported by regulators, provided that deployment is transparent and well-governed.

The Cost of Compliance

The cost of compliance is material. A study by Lexis Nexis and Oxford Economics in 2023 estimated banks' cost of complying with AML regulations in the United Kingdom to be £34.5 billion a year, double the £17.4 billion the government spends on policing all other crimes put together.[1]

This is an average cost of £220 a year to each of the UK banks' roughly 160 million customers, which includes not only British individuals but also some foreign individuals and both British and foreign companies.[1]

Moreover this amount is increasing. According to a 2024 PwC survey, 65% of UK financial institutions reported increased AML/KYC (Anti money laundering / know your customer) spending in the preceding two years.[2]

In another survey, PwC suggested that around the world the cost of just the account setup – ie the initial KYC - for a typical corporate customer could be as much as $311 (£230), while for regular clients it's closer to $12 (£9).

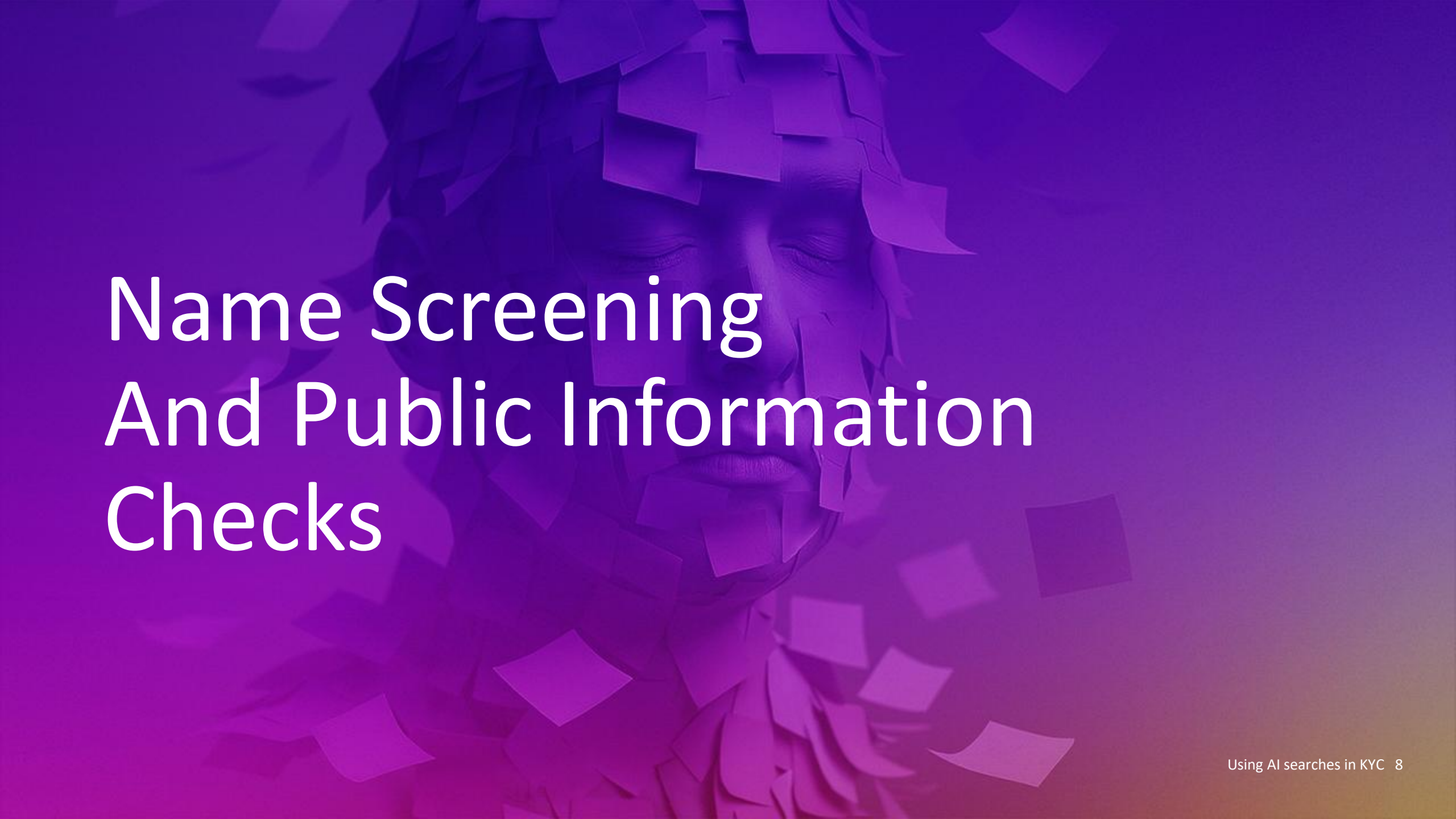
PwC then went on to provide a breakdown for the KYC costs of a corporate account as follows:

- Document validity and collection – $14 (£10)
- Publicly available information – $42 (£31)
- Screening – $77 (£57)
- Complete requirements – $81 (£60)
- Four-eye review – $93 (£69)
- Approval – $4 (£3) [3]

While some may quibble at the monetary costs, few would argue that this breakdown is not representative of the key KYC processes faced by the financial institutions and their impact on costs – in terms of systems, people and processes.

In another survey, Fenergo have looked at just the manpower needed to manage all this compliance. In their survey, one-third of all banks employ 1,000–1,500 full-time KYC staff, another third 1,501–2,000 such staff and the largest banks up to 3,000 employees dedicated solely to KYC operations.[4]

1. Reported by the Institute of Economic Affairs - https://iea.org.uk/publications/debanked-the-economic-and-social-consequences-of-anti-money-laundering-regulation/#
2. https://www.pwc.co.uk/financial-services/assets/pdf/emea-aml-survey-2024.html.pdf
3. https://www.pwc.com/sg/en/consulting/assets/pkyc-a-new-approach-to-periodic-reviews.pdf - These figures are based on global averages, rather than being specific to the United Kingdom.
4. https://resources.fenergo.com/blogs/the-cost-of-kyc-compliance-in-finance-how-digitalization-helps



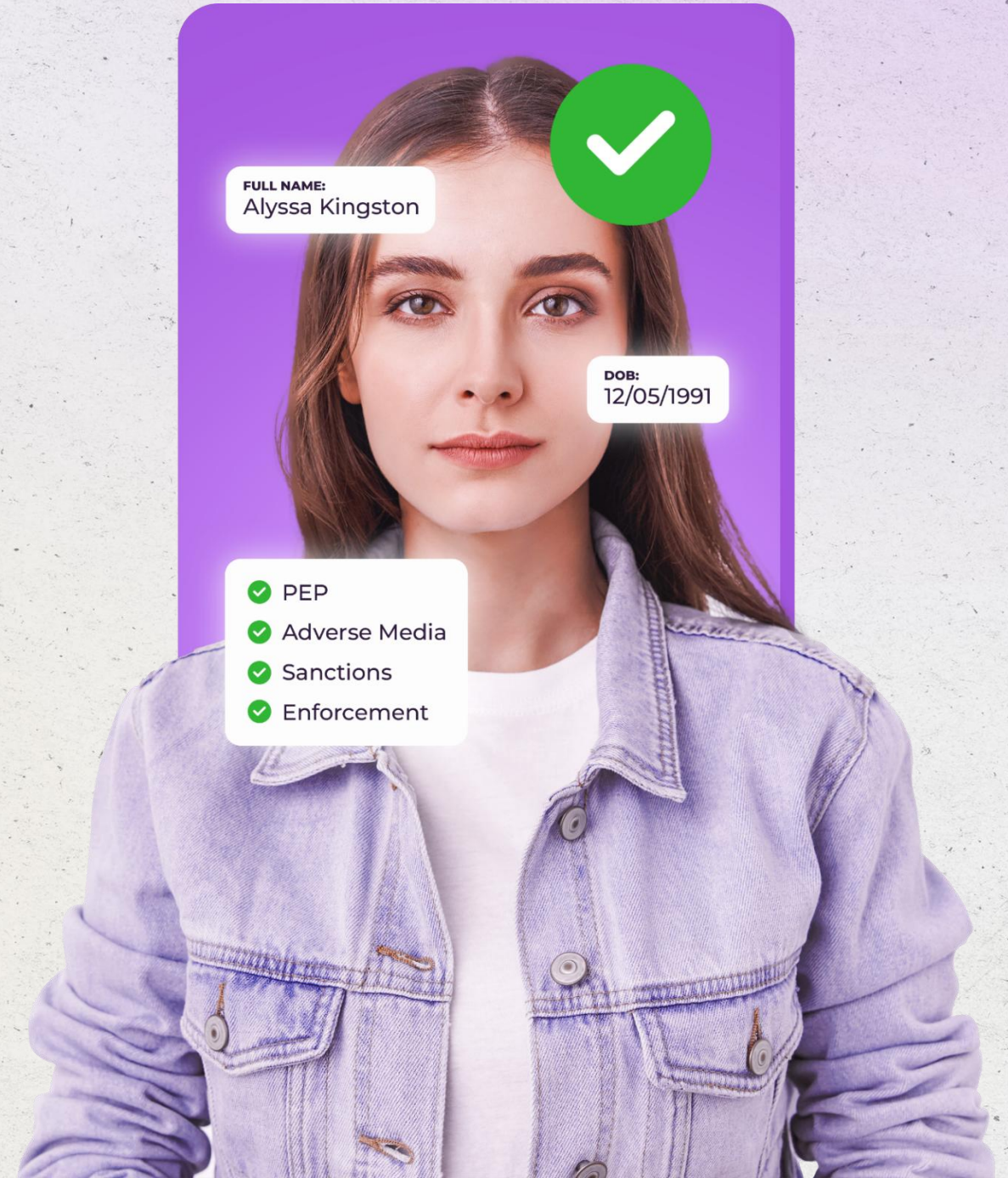
Name Screening And Public Information Checks

If we drill into these figures above, we see a large proportion of the total cost is related to name screening and Public Information Checks. Both
of these areas have grown into veritable cottage industries and a key process within any bank.

Name screening in KYC is the process where regulated institutions check the names of individuals or organisations against various databases to identify potential risks related to financial crimes, fraud, or regulatory restrictions.

Typically, these databases consist of the following categories –

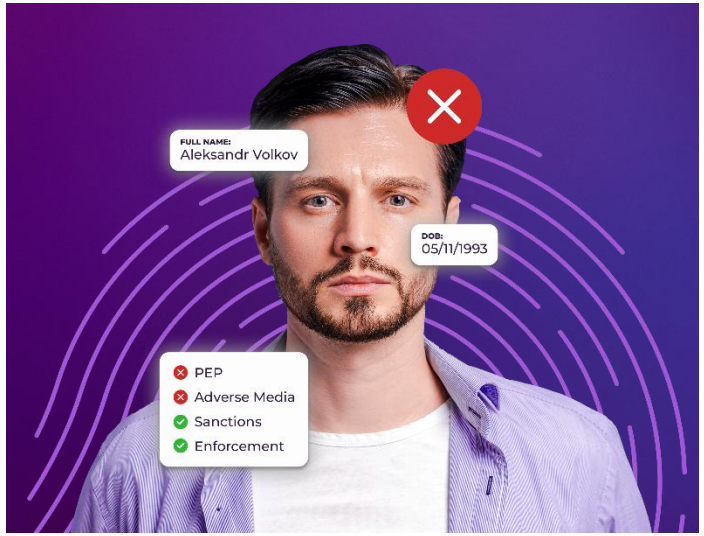
- Sanction Lists
- PEP / RCA lists
- Special Interest Lists



Sanction Lists

These are lists of terrorists and other criminals. If an individual or organisation is found on one of these lists, the regulated institution will typically deny them an account and also raise an STR (Suspicious Transaction Report) against them. Example Sanction lists include

- ✓ United Kingdom HM Treasury consolidated list
- ✓ European Union consolidated sanctions list
- ✓ United Nations security council sanctions list
- ✓ United States OFAC consolidated list

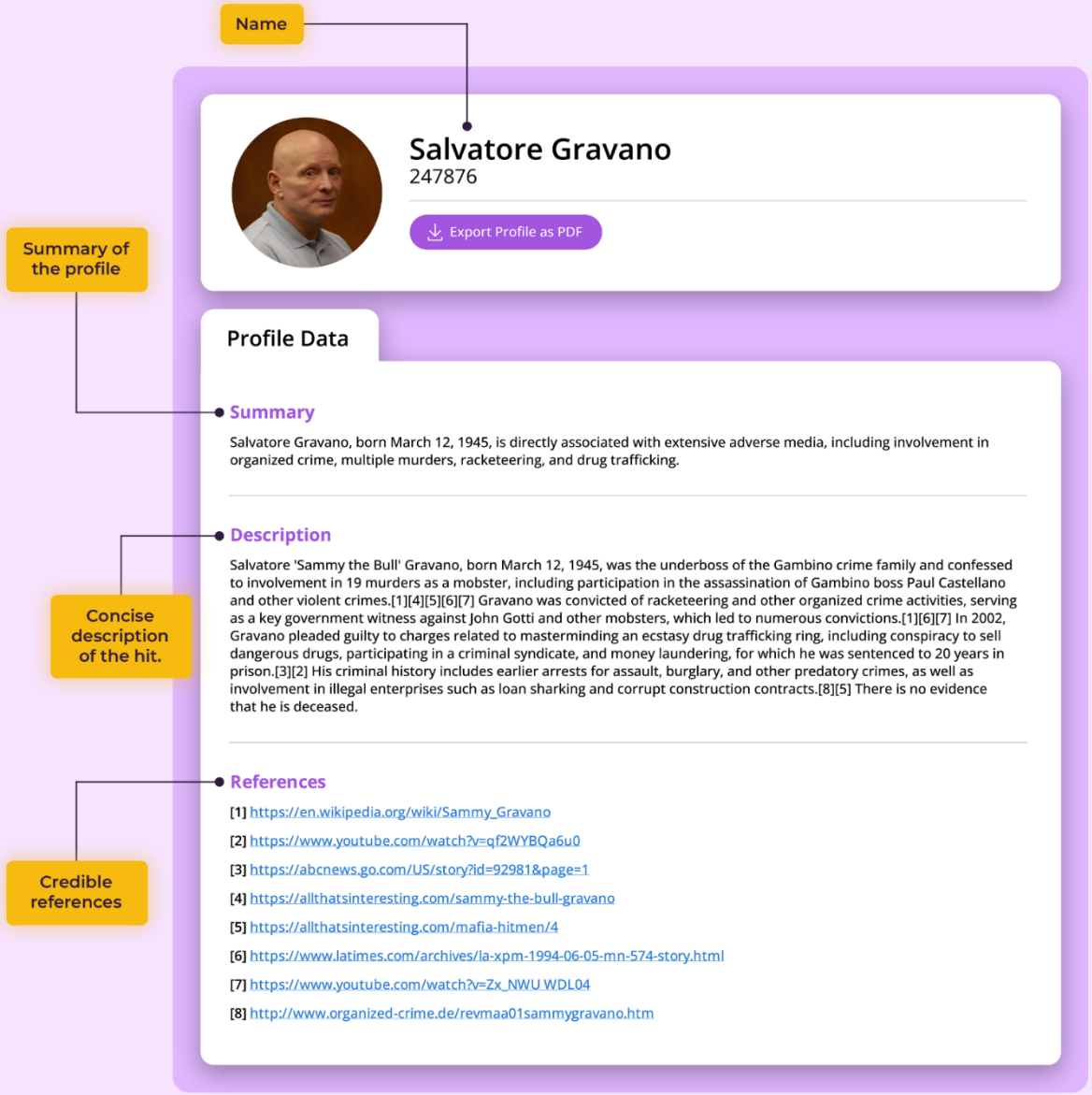


PEP / RCA lists

PEP stands for “Politically Exposed Person”. RCA stands for “Relatives and Close Associates”. Many high-profile people are on these PEP lists including politicians, high court judges and ambassadors. FATF (Financial Action Task Force) regards such people as high risk and so subject to Enhanced Due Diligence (EDD) and software vendors for regulated institutions therefore go to great length to compile lists of PEPs from every country around the world. PEP hits are not applicable for Companies.

Special Interest Lists

These lists collate data from exclusion, law and regulatory sources from around the world to identify individuals who have been found guilty of various crimes or misdemeanours and so should be flagged accordingly. Such customer will also be considered either high risk and so subject to EDD or in egregious cases denied an account with an STR raised.



Such screening of databases is however no longer considered sufficient by many regulators.

As KYC is a 360-degree process, screening alone is constrained by the finite nature of the databases despite their general comprehensiveness.

Databases can get stale. A general election for example may mean many 100s of new Members of Parliament. Crimes are constantly being reported and enforcement lists may not be full up-to-date.

To deal with this limitation, additional Public searches of Available Information are typically also required.

These focus specifically on 2 areas:

- **An Adverse Media check:** This focuses on negative news about a customer including matters that could cause reputational harm. Included within such checks are whether the customer has been involved in fraudulent or illegal activity connected with money laundering. This also helps touch customers who have been on the periphery of sanctionable activity.
- **An additional PEP check:** This focuses on customers who may not be on official PEP lists (which vary considerably around the world in breadth and quality), particularly those who may be in judiciary, military or civil service positions away from the usually expected politicians.

All these public internet checks take time and money.

To return to the PwC survey providing the breakdown of KYC costs per client, one of the sections is directly attributable to the reviewing of publicly available information.

Moreover indirectly a large proportion of completing requirements and the four-eyed review is also related to such checks

If we assume ¼ of requirement and four-eyed reviews time taken by such public searches (the other ¾ consisting of identity checks, name screening and risk assessments) it could be estimated that around 28% of total KYC costs are related to public internet checks.

Please reference the table on the right.

KYC Component	Total cost to a typical financial institution	Total cost attributable to public internet searches
Document validity and collection	£10	£0
Publicly available information	£31	£31
Screening	£57	£0
Complete requirements	£60	£15
Four-eye review	£69	£17
Approval	£3	£0
TOTAL	£230	£63 (28%)

Public searches is therefore a very large cost being borne by financial institutions.

The challenge with Public Searches

The key issue with public searches is the amount of work that has to go into them.

Let's look at a typical KYC flow to understand this better –

- The customer submits various information about themselves (eg their name, date of birth and nationality during KYC on-boarding. An image of them via a passport photo or a driving licence is also collected.
- Those name details are then placed in a public search engine. Some searches are loaded with particular key words (for example fraud, trafficker, criminal in the case of adverse media) to see if a connection with a genuine negative news story can be found.
- If a story or stories are found, the article(s) must be read by a compliance agent to determine whether the prospective customer is actually subject to negative news. For example if the customer's name is John Smith, there is a big difference between an article saying "John Smith was found guilty of fraud," and "John Smith accused his neighbour of fraud."

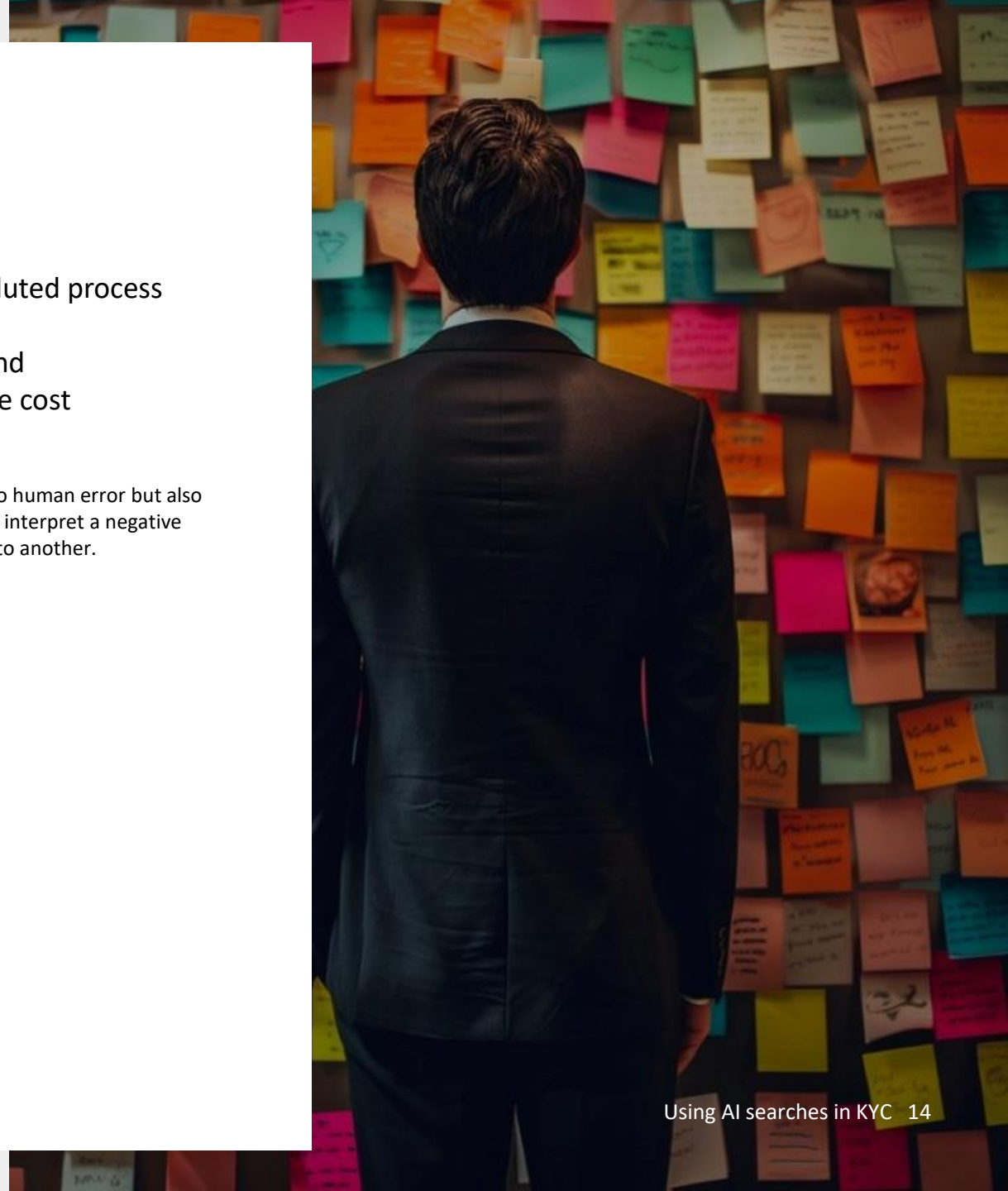
- Once it has been established if this is a genuine case of adverse media, the agent must check that the article is about the same person as the customer. This can be particularly tricky for common names like John Smith, so additional enhanced checking may need to be performed. The passport photo could be used if a photo of the individual in question is in the news article, but often additional checks may also be required.

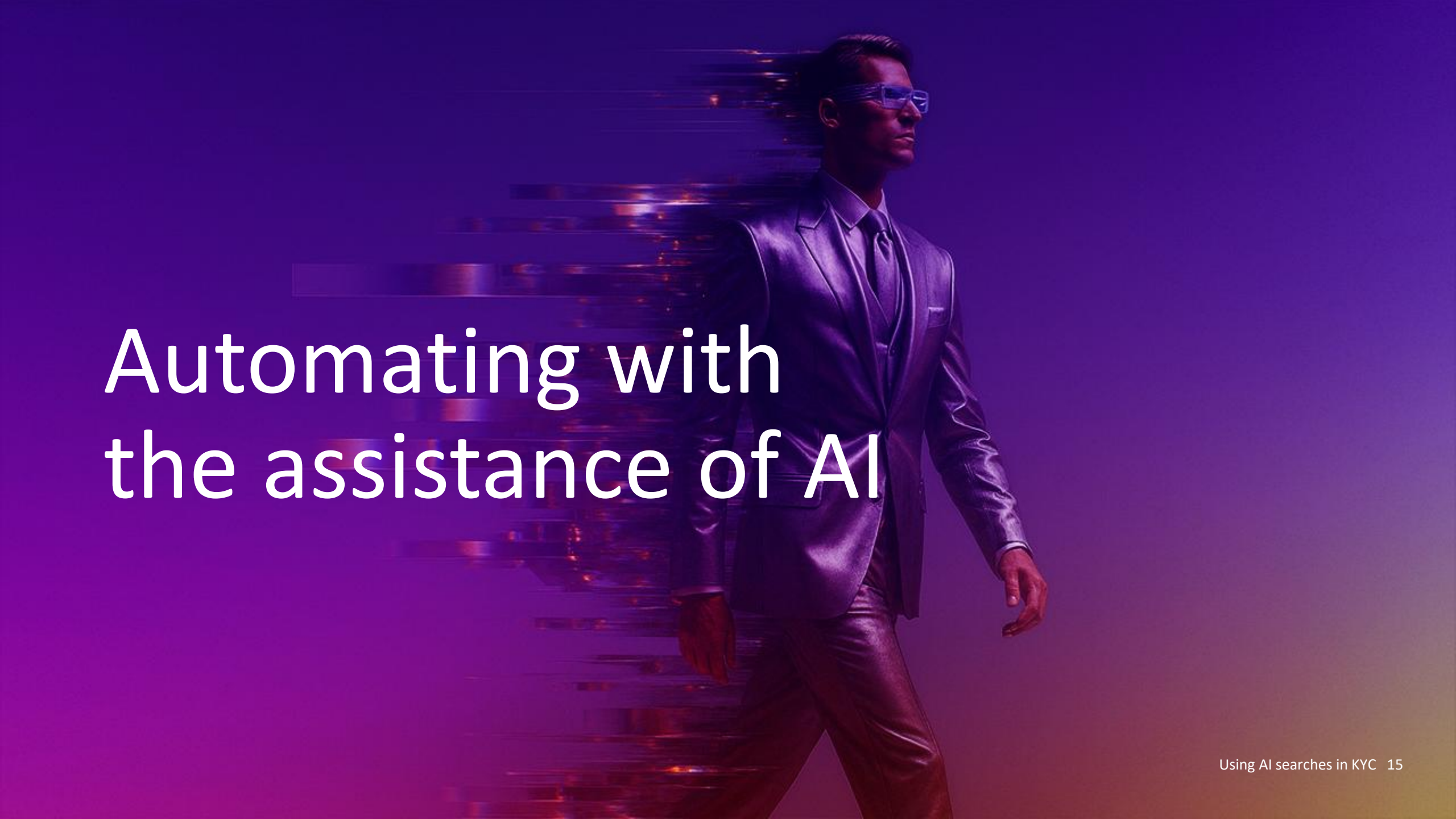
- A further complication is that news stories do evolve over time. So first “John Smith” may be accused of fraud. Next he goes on trial. Finally he is exonerated. So a full picture of the time line needs to be established before a decision can be made. In this case, “John Smith” was accused but found not-guilty, so this should no longer be a piece of negative news.

- The agent has to compile all of this into a report which would then be reviewed by a second person who is the the second half of the four eye review.

In summary this is a convoluted process with a lot of investigation, back and forth, checking and re-checking. No wonder the cost can be so high.

Moreover, it can be subject not just to human error but also human inconsistency. One agent may interpret a negative news story in a slightly different way to another.





Automating with the assistance of AI

At Idenfo, we believe that assessing publicly available information is a key area of compliance where AI could provide a very beneficial role in speeding up KYC decisions, ensure greater consistency in decision making and reduce overall compliance costs.

The challenge of course is how much can we trust AI to perform such a critical compliance role for us.

Use of such technology needs to be backed by deep compliance expertise to ensure that the results are accurate, consistent and relevant.

Idenfo's Intelligent Search is an advanced screening engine that combines the power of AI technology with deep compliance expertise. Idenfo was formed by compliance experts who understand compliance requirements and challenges and use technology to solution them.

Intelligent Search does not use any static databases or name screening lists, but instead performs a live web search to search for evidence associated with the entity in question that supports or refutes the fact that they are a PEP or are the subject of Adverse Media.

The system is powered by a large language model that is integrated with a search function and fine-tuned to provide evidence-based responses to the KYC inputs.

Through extensive testing and prompt engineering, we have developed a set of prompts, which, together with pre- and post-processing steps, are able to reliably produce high-quality Adverse Media and PEP screening results.

Static system prompts which describe the tasks at hand and how to go about them are combined with dynamic prompts which describe the entity being searched and instruct the model to initiate a search.

The prompts are detailed and lengthy, but broadly speaking, they each:

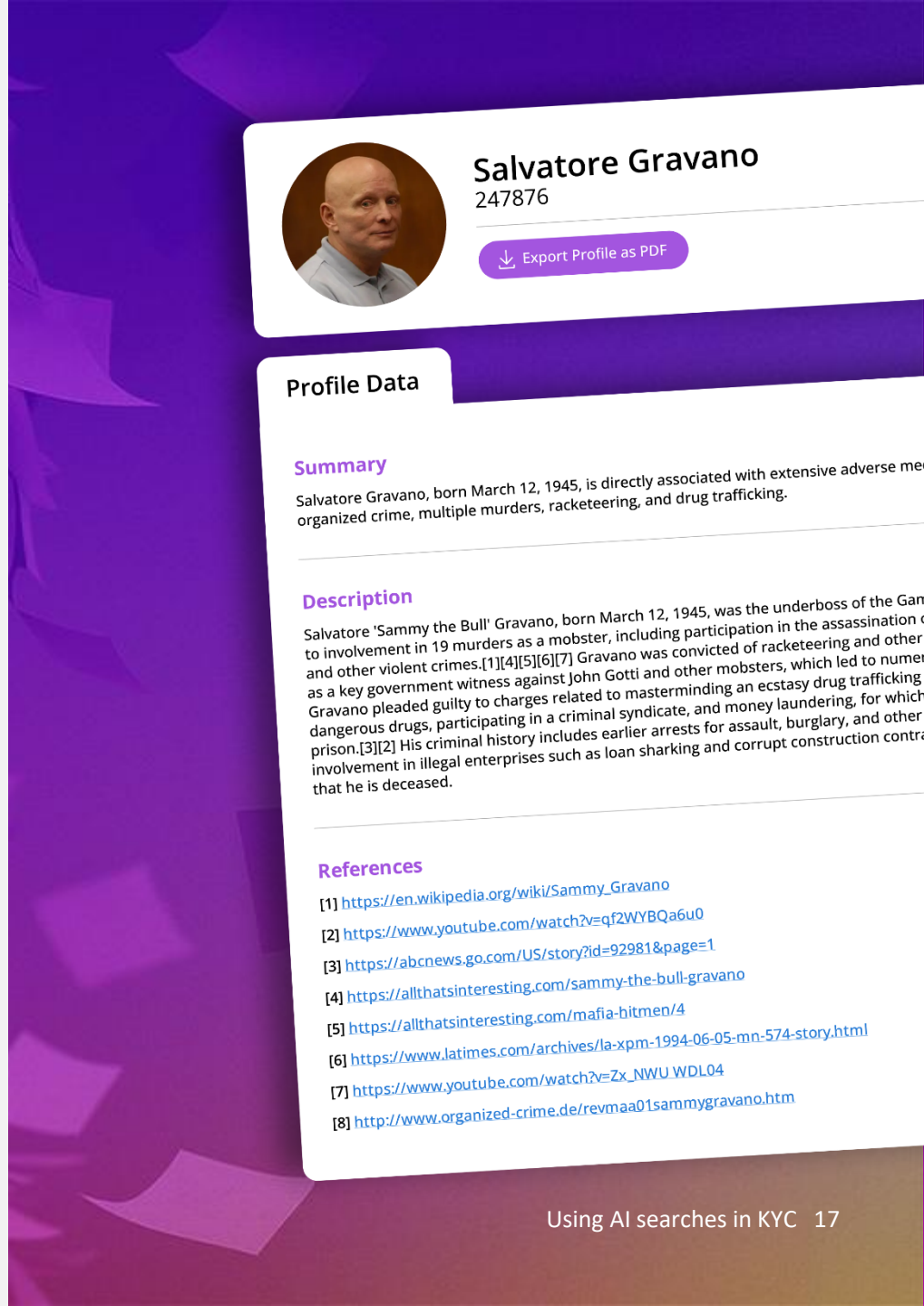
- Define relevant terms.
- Establish conditions for what should be considered Adverse Media or what constitutes a PEP. These are based on quantifiable yardsticks based on global regulatory frameworks.

  For example types of PEPs (politicians, civil servants, high court judges) are defined within the prompts. In Adverse Media, the difference between types of financial crime and their seriousness are also fully defined.

- Provide guidelines for how the model should analyse the collected evidence and come to a decision on an overall outcome.
- Define the required structured format for the model's response.

For each category (Adverse Media /PEP), Intelligent Search produces several outputs which provide direct benefits to the compliance team:

Outputs	Benefits
An holistic true/false outcome decision, indicating overall whether the entity has been determined to be a PEP or the subject of Adverse Media. This determination is based on the AI assessing all the available KYC information (including location relevance, age and profile data and broader context) as well as determining from the tone, manner and nature of the relevant matched articles.	The AI is therefore making a judgement call. It is acting as a “maker” within the four eye review process. This judgement is done within a matter of seconds and is fully automated. Its decision can of course be checked by the “checker” and overruled if necessary.
A one-line summary of the relevant evidence found to support the outcome.	This helps senior compliance staff, senior management, internal and external auditors see at a glance the results of an enquiry.
Detailed textual overview describing each piece of relevant information in more detail in order to create a clear, concise biography. For example, if evidence was found associating a PEP with two different positions, these would each be described separately. (see Figures 2 & 3 below)	PEP and Adverse Media searches are rarely straightforward. So the AI engine knows to systematically analyse each piece of evidence and list all of them down. Crucially the AI performs this analysis in a consistent manner. This ensures all Adverse Media and PEP hits are subject to the same consistent compliance framework.
A numbered list of URLs which link to the supporting evidence found to enable deeper checks to take place. Crucially, the numbered URLs are cited by the other outputs, directly linking the analysis to evidence.	All evidence is consolidated in one hit. So a compliance checker can review everything on one page rather than having to go through multiple tabs with single URL references on each. This speeds up the job for the checker and reduces overall compliance costs.



Summary

The case for using AI in KYC onboarding is overwhelming. This is not just due to its ability to check the ever-rising compliance costs but for its ability to provide a host of other related benefits –

- Regulations require ongoing screening and public searches to mitigate AML risks. This is already an enormous challenge, but detecting minor anomalies and assessing them in real-time against evolving risk profiles is nearly impossible without AI.
- Frequent repetitive public search checks mean compliance agents are often bogged down by low-value tasks, leaving less time for serious investigations. AI led process automation can handle these tasks efficiently, freeing compliance teams to focus on high-risk cases and strategic initiatives.
- Real-time compliance demands dynamic risk scoring and the ability to trigger perpetual KYC updates when risk profiles change such as a PEP update or an Adverse Media change. These are data-intensive, high-volume processes that AI can manage instantly, whereas manual processing would consume excessive human resources.
- The use of AI can also dramatically reduce the volume of false positive alerts and so improve overall compliance operational efficiency.

Compliance regulators broadly support the use of AI in financial services, but expect firms to ensure strong governance and transparency in its deployment.[5]

The Idenfo Intelligent Search solution provides a strong consistent framework for public Adverse Media and PEP searching. It can act as an add-on module for any regulated institution to run alongside existing name screening engines. It has the ability to streamline compliance checks by providing accurate, efficient and reliable results. This speeds up KYC decisions, ensures greater consistency in decision making and reduces overall compliance costs.

5. See the following for the government's key principles - https://www.gov.uk/government/publications/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators

About IDENFO

At Idenfo, we want to be ‘culturally remarkable’. We want to stand out from the crowd of FinTech startups and be known for the value we add not just to our businesses, but to our communities and the lives of the people we associate with.

We are driven by a desire to shape a better, safer world through technology.

We are driven by a desire to produce a net positive change in our societies. We understand that the work we do helps strengthen communities and make them safer and more stable, and this devotion to goodness is what makes our work meaningful. This is our societal purpose.

As a tech company, our purpose is to change the way digital financial technologies function in order to make them more secure. We aim to cause disruption and revolutionise the tech sphere with radical and original responses to improve digital security.

For more information, visit www.idenfo.com

Connect with us

facebook.com/IdenfoAML

linkedin.com/company/idenfo

instagram.com/idenfoaml

IDENFO

Bankside 300 Peachman Way,
Broadland Business Park, Norwich, Norfolk,
United Kingdom, NR7 0LB